



Koen Hampsink

Afstudeerverslag

Classificatie: Vertrouwelijk

Datum: 18 juni 2023 Versie: 2.0

© Copyright Exite ICT B.V., Enschede, 18 juni 2023

Behoudens strikt intern gebruik, voor het in de inleiding van dit document beschreven doel, mag niets uit deze uitgave, feitelijk of in afgeleide vorm, letterlijk of naar het idee, worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand of openbaar worden gemaakt door middel van druk, fotokopie, microfilm of op welke wijze ook, hetzij mechanisch, hetzij elektronisch, zonder voorafgaande schriftelijke toestemming van Exite ICT B.V.

Exite ICT B.V. heeft veel aandacht besteed aan het samenstellen van deze documentatie en is van mening dat de inhoud ervan correct is. Mochten echter om welke reden dan ook hierin onjuistheden voorkomen, zullen deze zo spoedig mogelijk worden hersteld.

Exite ICT B.V.

Postbus 331

7500 AH Enschede

+31 (0)88 399 22 00

info@exite.com

www.exite.com

Documentbeheer

Goedkeuring

Naam	Rol van Persoon	Goedkeuring
Koen Hampsink	Afstudeerder	
Don Hellwich	Afstudeerbegeleider Exite / opdrachtgever	
Herman Voortman	Afstudeerbegeleider Saxion	

Tabel 1 - Goedkeuring

Contactpersonen

Naam	E-mail	Rol van persoon
Koen Hampsink	484956@student.saxion.nl / k.hampsink@exite.com	Afstudeerder
Don Hellwich	d.hellwich@exite.com	Afstudeerbegeleider Exite / opdrachtgever
Herman Voortman	h.voortman@saxion.nl	Afstudeerbegeleider Saxion

Tabel 2 - Contactpersonen

Versiebeheer

Datum	Versie	Opmerking
18-6-2023	2.0	Definitief afstudeerverslag
9-6-2023	1.1	Verwerken feedback
4-6-2023	1.0	Concept afstudeerverslag
23-5-2023	0.5	Verwerken feedback
22-5-2023	0.4	Inleveren tussentijdse documentatie
10-5-2023	0.3	Verwerken feedback
5-5-2023	0.2	Inleveren tussentijdse documentatie
3-3-2023	0.1	Opzet document

Tabel 3 - Versiebeheer

Voorwoord

Voor u ligt het afstudeerverslag van het afstudeertraject van de opleiding HBO-ICT IT Service Management op Saxion te Enschede. Dit afstudeerverslag is geschreven in opdracht van Exite.

Het onderzoek is uitgevoerd in de periode februari tot juni bij Exite te Enschede. De kennis die ik heb opgedaan gedurende de opleiding heb ik kunnen toepassen in dit onderzoek.

Ik wil de bedrijfsbegeleider bedanken voor de betrokkenheid en begeleiding vanuit Exite. Ook voor alle tijd die hij genomen heeft om documentatie te controleren en vragen te beantwoorden. De begeleiding was goed en als prettig ervaren.

Verder wil ik de afstudeerbegeleider bedanken voor de begeleiding en feedback vanuit Saxion. Met deze feedback kon ik altijd verder werken aan het onderzoek.

Ik wens u veel leesplezier.

Figuren en tabellenlijst

Figuur 1 - Stakeholderanalyse	13
Figuur 2 - Public cloud.....	27
Figuur 3 - Private cloud.....	28
Figuur 4 - Hybride cloud	29
Figuur 5 - 6R strategie.....	30
Figuur 6 - Automatisch schalen.....	33
Figuur 7 - Motieven cloudmigraties	39
Figuur 8 - Vergelijking NAS	40
Figuur 9 - Remote Desktop Services.....	41
Figuur 10 - Citrix.....	42
Figuur 11 - Huidige situatie	47
Figuur 12 - Hybride Joined	49
Figuur 13 - Azure AD Joined.....	49
Figuur 14 - Microsoft SharePoint Migration Tool.....	51
Figuur 15 - Migratie Wasabi Cloud NAS.....	52
Figuur 16 - Prioritering stakeholders	71
Figuur 17 - Actieve Citrix omgeving.....	86
Figuur 18 - Citrix licenties.....	87
Figuur 19 - RDS licenties	88
Figuur 20- Nieuwe situatie.....	91
Tabel 1 - Goedkeuring.....	2
Tabel 2 - Contactpersonen	2
Tabel 3 - Versiebeheer	2
Tabel 4 - Stakeholders	14
Tabel 5 - Deelvragen.....	17
Tabel 6 - Randvoorwaarden	20
Tabel 7 - Business requirements	22
Tabel 8 - User requirements.....	23
Tabel 9 - System requirements	24

Tabel 10 - Ontwerpprincipes.....	42
Tabel 11 - Ontwerpprincipes.....	44
Tabel 12 - Verouderde servers.....	45
Tabel 13 - Huidige serverlandschap.....	46
Tabel 14 - Vereiste configuraties Intune.....	48
Tabel 15 - Optionele configuraties Intune.....	49
Tabel 16 - Citrix servers.....	52
Tabel 17 - RDS server.....	52
Tabel 18 - Nieuw serverlandschap.....	53
Tabel 19 - Af te schalen resources.....	55
Tabel 20 - Af te schalen servers.....	55
Tabel 21 - Te vervangen servers.....	58
Tabel 22 - Uitsfaseren Citrix.....	58
Tabel 23 - Ontwerpevaluatie.....	61
Tabel 24 - Interne- en externe stakeholders.....	70
Tabel 25 - Categorisering stakeholders.....	71
Tabel 26 - Stakeholders.....	72
Tabel 27 - Citrix omgeving.....	86
Tabel 28 - Licenties.....	90
Tabel 29 - Overige verouderde servers.....	90

Managementsamenvatting

Exite ICT is een IT-bedrijf dat diensten aanbiedt op het gebied van IT-infrastructuur, cloudoplossingen, cybersecurity en managed services. Exite heeft gevraagd onderzoek te doen naar de mogelijkheden om een complexe on-premise omgeving te optimaliseren dan wel migreren naar een public en/of hybride cloud. Gedurende dit onderzoek wordt antwoord gegeven op de hoofdvraag:

“Hoe kan Exite de IT-infrastructuur van een klant optimaliseren en migreren naar de cloud, hoe zal deze migratie moeten verlopen en wat zijn de gevolgen daarvan?”

Met behulp van de opgestelde deelvragen moet de hoofdvraag ondersteund worden.

In de probleemanalyse wordt duidelijk wat het probleem is. Daaruit blijkt dat een klant opnieuw moet investeren in hardware, omdat de support- en garantiecontracten op korte termijn verlopen. Er moet onderzocht worden of een migratie naar de cloud een passende oplossing is en hoe de migratie zal moeten verlopen. Beveiliging is daarbij een belangrijk onderdeel. Uit de stakeholderanalyse is gebleken dat de opdrachtgever, de customer succes manager en de klant de belangrijkste stakeholders zijn binnen dit onderzoek. Verder wordt in de contextanalyse vier randvoorwaarden opgesteld. De oplossing moet gebaseerd zijn op Microsoft technologie. Beveiliging moet voldoen aan de baselines van Exite met betrekking tot device security. Omgevingen welke te veel afhankelijk zijn van on-premise infrastructuur, worden niet gemigreerd en de oplossing moet gebaseerd zijn op producten en diensten welke momenteel al geleverd worden door Exite. In de behoefteanalyse zijn de eisen en wensen van de stakeholders in kaart gebracht. Denk hierbij aan het verkrijgen van inzicht van de huidige omgeving en dit om te zetten naar een ontwerp en advies. Uit het literatuuronderzoek is gebleken dat wanneer Exite de oplossing schaalbaar wilt maken de resources gemakkelijk aangepast moeten worden. Als het samenwerken in documenten mogelijk moet zijn, moet Exite centrale opslag van data inrichten voor klanten. Verder moet Exite Intune inrichten op basis van de gestelde eisen, om de beveiliging naar een minimaal niveau. Ook moet Exite rekening houden met best practices op het gebied van beveiliging. Om on-premise omgeving te optimaliseren en migreren moet Exite de omgeving goed in kaart brengen en eenvoudig opzetten.

In het ontwerp is inzicht verkregen in de huidige situatie en hoe Exite de nieuwe situatie moet inrichten. In de ontwerpevaluatie wordt beschreven hoe de eerder opgestelde requirements zijn behaald.

In het advies word beschreven op welke wijze Exite de oplossing moet implementeren met verschillende afwegingen. Verder wordt in het advies duidelijk welk vervolgonderzoek benodigd is om klanten specifiek verder te kunnen helpen naar de cloud.

Het antwoord dat op de hoofdvraag wordt gegeven is: Om de IT-infrastructuur van een klant te optimaliseren en naar de cloud te migreren, is het belangrijk om de huidige omgeving en werkwijze in kaart te brengen. Daarna moet bepaald worden welk type cloudoplossing het beste bij de klant past. Het is aangetoond dat een cloudmigratie het beste in behapbare fases kan worden uitgevoerd, zodat eindgebruikers geleidelijk kunnen wennen aan en leren werken in de cloud.

Inhoud

1	Inleiding.....	9
1.1	Achtergrond.....	9
2	Onderzoeksmethodieken	11
3	Probleemanalyse	12
3.1	Methodiek.....	12
3.2	Resultaten.....	13
3.3	Conclusie.....	17
4	Contextanalyse.....	18
4.1	Methodiek.....	18
4.2	Resultaten.....	19
4.3	Conclusie.....	20
5	Behoefteanalyse.....	21
5.1	Methodiek.....	21
5.2	Resultaten.....	21
5.3	Conclusie.....	24
6	Literatuuronderzoek.....	25
6.1	Methodiek.....	25
6.2	Resultaten.....	25
6.3	Conclusie.....	42
7	Ontwerp.....	43
7.1	Methodiek.....	43
7.2	Vereiste functionaliteiten.....	43
7.3	Huidige situatie	44
7.4	Nieuwe situatie.....	47
7.5	Conclusie.....	53
8	Advies.....	54
8.1	Methodiek.....	54
8.2	Resultaten.....	54
8.3	Advies en conclusie.....	59
9	Ontwerpevaluatie	61

10	Eindconclusie.....	62
10.1	Beantwoording deelvragen.....	62
10.2	Beantwoording hoofdvraag.....	64
10.3	Discussie.....	65
11	Reflectie.....	66
12	Bibliografie.....	67
13	Bijlagen.....	70
13.1	Bijlage A: Stakeholderanalyse.....	70
13.2	Bijlage B: Interviews.....	74
13.3	Bijlage C: Behoeftanalyse.....	82
13.4	Bijlage D: 7S-model.....	84
13.5	Bijlage E: Onderzoek huidige omgeving.....	86
13.6	Bijlage F: Nieuwe situatie.....	91

1 Inleiding

Dit document betreft de afstudeerscriptie van Koen Hampsink voor de opleiding HBO-ICT IT Service Management bij Hogeschool Saxion te Enschede. Het onderzoek is uitgevoerd in opdracht van Exite te Enschede. Exite heeft de wens om klanten met complexe on-premise omgevingen naar de cloud te brengen. In het onderzoek moet gekeken worden naar de mogelijkheden en vereisten om een klant naar de cloud te brengen, hoe deze migratie zal moeten verlopen en wat daar de gevolgen van zijn. Met behulp van het onderzoek is een ontwerp en advies beschreven, waarin de eisen en wensen van Exite zijn verwerkt.

Dit document is opgezet met behulp van de reader ontwerponderzoek van (Kai Haverman, 2022). In het onderzoek worden verschillende fases doorlopen om tot een gedegen advies te komen voor Exite. Gedurende deze fases wordt ook gebruik gemaakt van andere methodieken, welke beschreven staan in hoofdstuk 2, onderzoeksmethodieken.

Om de probleemstelling in kaart te brengen wordt er gestart met een probleemanalyse. Deze probleemanalyse is opgesteld vanuit verschillende perspectieven. Het uitvoeren van de probleemanalyse resulteert in een hoofdvraag, welke wordt ondersteund door verschillende deelvragen. De antwoorden op de deelvragen zullen het beantwoorden van de hoofdvraag ondersteunen. Na het uitvoeren van de probleemanalyse is er een contextanalyse opgesteld. In de contextanalyse is gekeken naar Exite als interne organisatie en Exite als externe organisatie. Hieruit komen een aantal randvoorwaarden. Vervolgens is er een behoefteanalyse opgesteld. In de behoefteanalyse zijn de eisen en wensen van de stakeholders in kaart gebracht, waar een lijst met requirements uit komt. Zodra de analyses zijn afgerond wordt er literatuuronderzoek opgesteld. In het literatuuronderzoek wordt gekeken naar algemene informatie omtrent cloudmigraties vanuit de literatuur en wordt er antwoord gegeven op een aantal deelvragen. Met behulp van het literatuuronderzoek kan er een gedegen ontwerp gemaakt worden.

Wanneer het literatuuronderzoek is afgerond wordt er een ontwerp gemaakt, waarin de eisen en wensen van Exite zitten verwerkt. In het ontwerp wordt gekeken hoe de huidige omgeving van de klant geoptimaliseerd en gemigreerd kan worden naar de cloud. In de ontwerpevaluatie zal vervolgens gekeken worden of de opgestelde requirements behaald zijn. De conclusies die uit het ontwerp komen zullen worden meegenomen in het advies, zodat er een gedegen advies gegeven kan worden aan Exite.

1.1 Achtergrond

Sinds 1998 maakt Exite impact met de slimme inzet van ICT-oplossingen en -diensten voor het grotere MKB. Van ICT-infrastructuur tot werkplekoplossingen en van datamanagement tot advies. Eerst als Sigmax ICT Specialisten en sinds 2019 als Exite (ICT).

Exite heeft meer dan 300 klanten van uiteenlopende branches tot diverse windstreken: vanuit Twente heeft Exite een klantportfolio opgebouwd waar ze graag voor werken en trots op zijn.

Met meer dan 140 collega's bestaande uit specialisten in disciplines als netwerk, datacenter, werkplek en beveiliging kunnen ze elk vraagstuk aan. Ook in ondersteunende rollen werken best-in-class professionals.

De ambitie van Exite is om de meest servicegerichte ICT-dienstverlener van NL te zijn, met de hoogste klantwaardering. In alles wat ze doen staat hospitality daarom centraal.

2 Onderzoeksmethodieken

Gedurende het onderzoek wordt er gebruik gemaakt van verschillende onderzoeksmethodieken. Dit zorgt ervoor dat het onderzoek voldoende diepgang heeft. In dit hoofdstuk worden de gebruikte onderzoeksmethodieken beschreven.

Met onderzoek wordt er onderscheidt gemaakt tussen kwantitatief onderzoek en kwalitatief onderzoek.

“Kwantitatieve data worden uitgedrukt in getallen, tabellen, grafieken en diagrammen. Dit type onderzoek wordt gebruikt om theorieën en hypothesen te bevestigen of te verwerpen. Kwantitatief onderzoek kan worden ingezet om feiten te verzamelen die kunnen worden gegeneraliseerd naar een grotere populatie. Veelgebruikte kwantitatieve dataverzamelingsmethoden zijn experimenten, kwantitatieve observaties en enquêtes met gesloten vragen.” (Merkus, 2021)

“Kwalitatieve data hebben vaak de vorm van woorden. Dit type onderzoek wordt gebruikt om concepten, gedachten of ervaringen te begrijpen. Met kwalitatief onderzoek kun je inzicht verkrijgen in onderwerpen waar nog weinig kennis over is. Veelgebruikte kwalitatieve dataverzamelingsmethoden zijn interviews met open vragen, kwalitatieve observaties en literatuurstudies over concepten of theorieën.” (Merkus, 2021)

In dit onderzoek zal de focus gelegd worden op kwalitatief onderzoek. Er is veelal deskresearch gedaan in combinatie met het uitvoeren van interviews. Deze interviews zijn uitgevoerd in semigestructureerde vorm, om zowel de benodigde informatie te verschaffen als eventuele aanvullende informatie door de mogelijkheid tot doorvragen. (Merkus, Semigestructureerd of half-gestructureerd interview | Voorbeeld, 2021) (Krul, 2014)

Gedurende het onderzoek wordt er gewerkt naar het ontwerp en advies. Door Kai Haverman, Esther Hageraats en Steven van der Linden is een ontwerpmethodiek beschreven, genaamd onderzoekend ontwerpen. Deze ontwerpmethodiek zal gebruikt worden voor het analyseren en onderzoeken gedurende het afstudeertraject. Dit is ook terug te zien in de structuur van het afstudeerverslag. Deze methodiek wordt gebruikt als raamwerk, waarin ook andere methodieken aan te pas komen.

“Het is voor een HBO’er van belang dat hij/zij gericht de beroepscontext kan vaststellen en op systematische wijze onderzoek uit kan voeren. Het onderzoek is voor de professionals echter geen doel, maar een middel. De opleiding IT Service Management van Saxion wil hier vorm aan geven met een concrete methodiek die de professional ondersteunt. Wij (schrijver van de methodiek) geloven dat onze studenten hiermee een stevig stuk gereedschap in de handen hebben waarmee ze de uitdagende taken die de wereld voor ze heeft met succes kunnen vervullen.” (Kai Haverman, 2022)

3 Probleemanalyse

Voor het vaststellen van de vraag van Exite is een probleemanalyse uitgevoerd. Om deze probleemanalyse goed uit te voeren is er gebruik gemaakt van onderzoeksmethodieken, welke in de volgende paragraaf worden beschreven. Het doel van deze probleemanalyse is om de vraag van de opdrachtgever vast te stellen, vanuit de verschillende perspectieven.

3.1 Methodiek

Om een zo volledig mogelijke probleemstelling te formuleren, is het belangrijk om het probleem vanuit verschillende perspectieven te bekijken en zo de betrouwbaarheid van het onderzoek te verhogen (triangulatie).

Dit is gedaan vanuit het oogpunt van enkele stakeholders, nadat een longlist van mogelijke belanghebbenden bij het onderzoek was opgesteld. Deze lijst is gecategoriseerd op basis van stakeholdertype en geprioriteerd met behulp van de Mendelow-methode, die de stakeholders rangschikt op basis van hun belang en macht bij het project (Mendelow, 1991). De resulterende shortlist van stakeholders, die een hoge betrokkenheid hebben, verbetert de validiteit van het onderzoek door te voorkomen dat slecht geïnformeerde stakeholders betrokken zijn. De stakeholderanalyse is te vinden in bijlage A – Stakeholderanalyse. Om de probleemstelling zo goed mogelijk te formuleren, zijn verschillende perspectieven bekeken, waaronder die van de shortlist van stakeholders, de literatuur en de onderzoeker zelf.

3.1.1 Interviews

Allereerst wordt er vanuit het perspectief van de verschillende stakeholders op de shortlist gekeken. Voor elke stakeholder wordt er een interview afgenomen, waarbij er gebruik wordt gemaakt van een semigestructureerde aanpak.

Semigestructureerde interviews worden ook wel kwalitatieve interviews of diepte-interviews genoemd. Hierbij gebruik je een algemeen interviewschema met vooropgestelde, wat algemener geformuleerde, vragen, maar je mag hier wel van afwijken. Zo kun je bijvoorbeeld doorvragen als je respondent iets interessants zegt of als je niet helemaal begrijpt wat diegene bedoelt. Hiermee verkrijg je meer en gedetailleerde informatie, wat in kwalitatief onderzoek vaak het doel is. (Dingemanse, 2015)

Na het afnemen van de interviews met de stakeholders, wordt de probleemstelling opgesteld. Hierbij wordt rekening gehouden met het perspectief vanuit de literatuur en vanuit de onderzoeker, in aanvulling op de inzichten die zijn verkregen tijdens de interviews met de stakeholders. De uitwerking van de interviews zijn te vinden in bijlage B – Interviews. Voor het opstellen van de probleemstelling zijn de volgende personen met bijbehorende functie geïnterviewd:

- ✕ Solution Architect en tevens opdrachtgever
- ✕ Sales / Customer Success Manager
- ✕ Business Consultant & Security Officer
- ✕ Solution Architect

3.1.2 Deskresearch

Als aanvulling op de interviews wordt er deskresearch uitgevoerd, in de vorm van literatuuronderzoek. Hierdoor kan het literatuurperspectief worden bepaald.

3.2 Resultaten

In dit hoofdstuk worden de resultaten beschreven van de probleemanalyse.

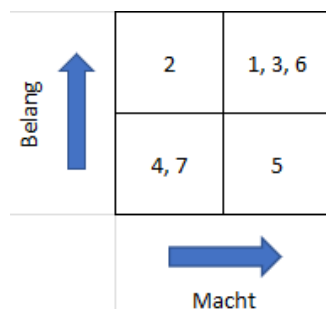
3.2.1 Stakeholderanalyse

Om tot de complete probleemstelling te komen en de juiste selectie van stakeholders, is er een stakeholderanalyse uitgevoerd. Deze is te vinden in bijlage A – Stakeholderanalyse. De resultaten daarvan zullen hier kort worden toegelicht.

Allereerst is er met de opdrachtgever gesproken omtrent het onderwerp van het onderzoek. Gedurende deze gesprekken is er een longlist van stakeholders opgesteld, welke bestaat uit onderstaande stakeholders:

- ✕ Exite ICT
- ✕ Solution Architect(en) Exite
- ✕ Customer Success Manager Exite
- ✕ Manager beheer Exite
- ✕ Security Officer Exite
- ✕ Klant
- ✕ Leveranciers Exite

Na deze eerste inventarisatie zijn bovenstaande stakeholders gecategoriseerd in interne- en externe stakeholders. Na het categoriseren is er gekeken naar welke stakeholders direct of indirect invloed hebben op het onderzoek. Hierdoor kunnen de stakeholders geprioriteerd worden wat resulteert in onderstaande resultaten:



Figuur 1 – Stakeholderanalyse

Stakeholders met een hoge score op basis van macht en belang worden automatisch toegevoegd aan de shortlist van stakeholders.

In onderstaande tabel worden de stakeholders toegelicht.

Nr.	Stakeholder	Toelichting
1	Exite ICT	Exite heeft als opdrachtgever een hoge macht en groot belang bij dit project. Om dit perspectief te beschrijven is het uitgangspunt gebruikt van een Solution Architect.
2	Solution Architecten Exite	De solution architecten binnen Exite hebben een groot belang bij het project, aangezien zij oplossingen ontwerpen en beheren voor klanten. Ook hebben zij veel macht, zij maken belangrijke afwegingen en adviseren hierin.
3	Customer Success Manager Exite	De customer success managers hebben veel belang bij het project, maar minder macht. Zij zijn verantwoordelijk om de eisen en wensen van de klant goed in kaart te brengen en willen de klant tevreden stellen.
4	Manager Beheer Exite	De manager beheer heeft zowel minder belang als minder macht bij het project. Hij/zij voert geen directe werkzaamheden uit bij klanten.
5	Security Officer Exite	De security officer heeft wat minder belang en veel macht bij het project. Hij/zij is verantwoordelijk voor de beveiliging van zowel nieuwe als bestaande oplossingen.
6	Klant	De klant heeft een groot belang bij het project. Zij gaan immers gebruik maken van de oplossing. Omdat het externe stakeholders zijn hebben zij geen directe invloed.
7	Leveranciers Exite	Leveranciers hebben geen directe macht bij het project. Exite is afhankelijk van leveranciers, maar kan kiezen voor een andere leverancier. Leveranciers hebben geen belang bij het resultaat van het project.

Tabel 4 –Stakeholders

3.2.2 Probleemstelling

Om tot een complete probleemstelling te komen is gesproken met onderstaande stakeholders:

- ✕ Opdrachtgever (Solution Architect)
- ✕ Customer Success Manager
- ✕ Security Officer
- ✕ Klant

De toedracht van de opdracht is dat de klant opnieuw moet gaan investeren in hardware, aangezien de support en garantie contracten bij leveranciers op korte termijn gaan verlopen.

Er moet worden onderzocht worden of een migratie naar de cloud een passende oplossing is en hoe deze migratie zal moeten verlopen. Ook moet onderzocht worden welk type cloudoplossing het beste past voor deze situatie (hybride, public, private etc.). Daarbij is het belangrijk om uitgebreid onderzoek te doen naar de beveiligingseisen. Ook moet er gekeken worden naar welke applicaties er draaien en of/hoe deze gemigreerd kunnen worden naar een passende cloudoplossing. Hier zal ook een advies voor beschreven moeten worden. Dit advies is terug te vinden in hoofdstuk 9 van dit document.

De klant maakt gebruik van een aantal applicaties die gebaseerd zijn op een client/server model. De klant heeft momenteel ook een traditionele telefonie oplossing waar ze in de toekomst naar willen kijken.

3.2.3 Literatuurperspectief

Na het uitwerken van de probleemstelling is gekeken naar de exacte definitie van een cloudmigratie. Microsoft schrijft hier het volgende over: "Bij een cloudmigratie worden apps en gegevens van de ene locatie, vaak de privéservers op locatie ('on-premises') van een bedrijf naar de servers van een provider van een openbare cloud verplaatst, maar ook tussen verschillende clouds. De belangrijkste voordelen van een cloudmigratie zijn het verminderen van de IT-kosten en het verbeteren van de prestaties, maar ook op het gebied van beveiliging, gebruiksgemak en op andere gebieden biedt het voordelen." (Microsoft, 2023)

Ook heeft het National Institute of Standards and Technology's (NIST) een definitie beschreven omtrent cloud computing. Zij schrijven het volgende: "Cloud computing is een relatief nieuw bedrijfsmodel in de computertechnologie wereld. Volgens de officiële definitie van NIST is "cloud computing een model voor het mogelijk maken van alomtegenwoordige, handige, on-demand netwerktoegang tot een gedeelde pool van configureerbare computerbronnen (bijv. netwerken, servers, opslag, applicaties en services) die snel kunnen worden geleverd en vrijgegeven met minimale inspanning voor beheer of interactie met de serviceprovider." (NIST, 2011)

3.2.4 Perspectief opdrachtgever (Solution Architect)

De solution architect van Exite geeft aan dat hij vaak al betrokken is bij het presales traject bij projecten. Hij krijgt veel informatie van degene die de eerste gesprekken met de klant gevoerd heeft (customer success manager). Zodra het technisch wordt, zal hij verder aanhaken. Hij probeert een zo goed mogelijk technisch plaatje te schetsen van de eisen en wensen van de klant. Samen met de customer success manager zullen ze ervoor zorgen dat dit op de juiste manier bij de desbetreffende klant landt.

3.2.5 Perspectief Sales / Customer Success Manager

De customer success manager is verantwoordelijk voor het binden van nieuwe klanten aan Exite, relatiebeheer van bestaande klanten en het uitbreiden van klanten. Dit wordt gedaan door te adviseren in de keuzes die een klant heeft op het gebied van beveiliging, migratietrajecten en een nieuwe moderne werkplek. De customer success manager vindt het belangrijk dat je begint met kijken in welke situatie zit de klant nu, hoe werken ze nu en sluit dat aan bij wat ze willen. Vanuit daar kijken zij hoe ze de klant het beste kunnen faciliteren. Wanneer een plan wordt bedacht wat niet doelt op de juiste zaken gaat het vanaf daar al mis. Wat ook erg belangrijk is, is om voortdurend na te denken hoe je de adoptie gaat aanpakken, een stukje verandermanagement komt daarbij kijken.

3.2.6 Perspectief Business Consultant & Security Officer

Het perspectief van de security officer is dat de beveiliging van een omgeving afhankelijk is van de omvang van de scope. Als er bijvoorbeeld een 1-op-1 migratie naar Azure wordt uitgevoerd, kan de standaardbeveiliging van Azure al voldoende zijn. Echter, als er persoonlijke gegevens van de klant worden verwerkt, moeten er extra maatregelen worden genomen om deze gegevens te beschermen, zoals het versleutelen van de databases en het implementeren van extra technische controles.

Daarnaast moet er goed gekeken worden naar wie er toegang heeft tot de Azure-omgeving en de databases. Is dit alleen de klant of zijn er ook andere partijen die toegang hebben? Het is belangrijk om ervoor te zorgen dat de toegang goed beveiligd is, bijvoorbeeld met Multi Factor Authenticatie (MFA). Verder moeten alle logische stappen kritisch tegen het licht gehouden worden om te controleren of deze veilig zijn.

Ook de back-up is een belangrijk onderdeel van de beveiliging en moet goed worden opgeslagen, bijvoorbeeld binnen Azure of op een ander platform. Daarnaast moet er gekeken worden naar wie er toegang heeft tot de back-up en of deze personen hoge rechten hebben binnen de Azure-omgeving. Door goed na te denken over deze zaken en over security kunnen we een veilige omgeving opzetten voor onze klanten.

3.2.7 Perspectief klant

Om het probleem goed in kaart te brengen is er ook gekeken naar het perspectief van de klant. Zij geven aan dat er momenteel gebruik gemaakt wordt van een Citrix omgeving die draait op Windows Server 2012 R2. Deze besturingssystemen worden per oktober 2023 niet meer ondersteund.

Dat is dan ook de reden dat deze klant vraagt om te kijken naar een andere, vernieuwende oplossing. Het is gewenst om te kijken op welke manier de huidige omgeving geoptimaliseerd en gemigreerd kan worden naar een public/hybride cloudoplossing. Er zijn nog maar een paar gebruikers die gebruik maken van de huidige Citrix omgeving.

3.2.8 Perspectief onderzoeker

Nu de eerste probleemanalyses in dit hoofdstuk zijn beschreven, is het perspectief van de onderzoeker ook erg belangrijk. Cloudmigraties spelen een grote rol in deze tijd. Veel bedrijven willen hun IT uitbesteden, om zich te kunnen focussen op hun eigen core business. Wanneer een IT-omgeving van een bedrijf stil valt, kan dit grote gevolgen hebben voor de bedrijfsvoering. Ook beveiliging is enorm belangrijk. Gevoelige data moet veilig worden opgeslagen, zodat deze niet in verkeerde handen komt. Het beveiligingsperspectief wordt dan ook als erg belangrijk gezien door de onderzoeker. De onderzoeker herkent zich in de probleemstelling van de opdrachtgever.

3.3 Conclusie

3.3.1 Hoofdvraag

Op basis van bovenstaande probleemstelling is er een hoofdvraag geformuleerd. Om deze hoofdvraag te kunnen beantwoorden zijn er enkele deelvragen geformuleerd. De deelvragen zullen gedurende het onderzoek beantwoord worden. De hoofdvraag luidt:

Hoe kan Exite de IT-infrastructuur van een klant optimaliseren en migreren naar de cloud, hoe zal deze migratie moeten verlopen en wat zijn de gevolgen daarvan?

3.3.2 Deelvragen

Om de hoofdvraag goed te kunnen beantwoorden, zijn er deelvragen geformuleerd. De deelvragen geven uiteindelijk antwoord op de hoofdvraag.

Beroepsproduct	Deelvraag
Literatuuronderzoek	Wat is de definitie van cloudcomputing?
Literatuuronderzoek	Wat zijn de mogelijkheden met betrekking tot een migratie naar de cloud?
Literatuuronderzoek	Wat moet er gedaan worden om ervoor te zorgen dat de beveiliging in de cloud voldoende is?
Literatuuronderzoek	Hoe kan een cloudoplossing schaalbaar worden gemaakt?
Literatuuronderzoek	Welke gevolgen zou een migratie naar de cloud met zich mee brengen voor een klant?
Ontwerp	Wat is de huidige IT-infrastructuur van de klant?
Probleemanalyse	Wat zijn de huidige knelpunten op het gebied van beveiliging?
Literatuuronderzoek	Wat zijn de kritische succesfactoren om het project te doen slagen voor een klant?
Ontwerp & Advies	Hoe kan Exite de mogelijke cloudoplossing implementeren?

Tabel 5 - Deelvragen

4 Contextanalyse

Om de resultaten van dit onderzoek bruikbaar te maken voor Exite, worden er in dit hoofdstuk een aantal randvoorwaarden geformuleerd.

4.1 Methodiek

Om een lijst met randvoorwaarden op te stellen, is een contextanalyse uitgevoerd waarbij gekeken is naar de omgeving waarin de resultaten van het onderzoek gebruikt zullen worden. Om de interne context tot stand te brengen is het 7-S model van McKinsey (Schop, 2023) gebruikt, waarmee gekeken is naar Exite als organisatie. Dit is beschreven in bijlage D – 7S-model. Daarnaast is er voor de externe context de leveranciers, concurrenten en klanten van Exite onderzocht. Om informatie te verzamelen over de omgeving zijn interviews gehouden met stakeholders en zijn er documenten geanalyseerd.

4.1.1 Interviews

De uitgewerkte interviews zijn te vinden in bijlage B – Interviews. De methodiek voor het houden van interviews is beschreven in hoofdstuk 1.1 van de bijlage.

Om de contextanalyse op te stellen is er met enkele stakeholders gesproken. Met onderstaande stakeholders zijn gesprekken gevoerd omtrent de contextanalyse:

- ✕ Solution architect
- ✕ Customer success manager
- ✕ Security officer

De genoemde stakeholders zijn geïnterviewd, omdat deze stakeholders betrokken zijn bij dit project en benoemd zijn als interne stakeholders. Om tot deze samenstelling van stakeholders te komen is een stakeholderanalyse uitgevoerd, deze is terug te vinden in bijlage A – Stakeholderanalyse.

4.1.2 Document analyse

Ook zijn er interne documenten van Exite bekeken, waarin de missie en visie zijn benoemd (Exite ICT, 2023). Om concurrenten van Exite in kaart te brengen, is er online onderzoek gedaan naar IT-bedrijven welke soortgelijke diensten als Exite aanbieden.

4.2 Resultaten

De contextanalyse zal worden opgedeeld in een interne analyse en een externe analyse. In de externe analyse worden de leveranciers, klanten en concurrenten van Exite benoemd.

4.2.1 Interne analyse

Exite ICT is een IT-bedrijf dat diensten aanbiedt op het gebied van IT-infrastructuur, cloudoplossingen, cybersecurity en managed services. Exite heeft een missie om mens en organisatie te prikkelen om met slimme inzet van ICT hun maximale potentieel te benutten en impact te maken op de wereld van morgen. Hun visie is om mens en technologie in balans te brengen, waardoor organisaties in staat zijn om hun ongekende vermogens te realiseren en het beste uit zichzelf te halen.

Exite heeft een platte organisatiestructuur en gebruikt verschillende systemen om haar diensten te leveren. Exite heeft een team van hoogopgeleide IT-professionals in dienst die goed presteren en betrokken zijn bij de organisatie. De stijl van Exite is gericht op open communicatie, samenwerking en het delen van kennis en ervaring. Het bedrijf heeft expertise en vaardigheden op het gebied van IT-dienstverlening, projectmanagement en consultancy, maar er is ook ruimte voor uitbreiding van het dienstenaanbod om te kunnen voldoen aan de veranderende behoeften van klanten. Uitdagingen voor Exite zijn onder meer het aantrekken en behouden van talent in een competitieve markt en het uitbreiden van het dienstenaanbod om te kunnen voldoen aan de veranderende behoeften van klanten.

4.2.2 Externe analyse

Klanten Exite

Exite heeft meer dan 250 klanten en is actief voor zowel grote als kleine B2B organisaties. Van de bakker op de hoek tot de multinational met tientallen vestigingen: wij bedienen uiteenlopende organisaties in heel Nederland met slimme inzet van ICT. Hoewel we in vele sectoren thuis zijn, beschouwen we als specialist in ICT-oplossingen dienstverlening een vijftal branches als ons natuurlijke werkterrein (Exite ICT, 2023):

- ✕ Zakelijke dienstverlening
- ✕ Zorg
- ✕ Productie & Engineering
- ✕ (Semi)overheid
- ✕ Bouw & High-tech

Leveranciers Exite

Exite is actief in de IT-dienstverlening in verschillende branches en maakt gebruik van zowel nationale en internationale leveranciers voor het inkopen van producten en diensten. Bij voorkeur maakt Exite gebruik van standaardproducten van partnerleveranciers. Onderstaande leveranciers zijn erg belangrijk voor Exite:

- ✕ Microsoft
- ✕ N-Able / SolarWinds
- ✕ Cisco (Meraki)
- ✕ NetApp
- ✕ VMware
- ✕ Keenondots
- ✕ TD Synnex (voorheen Techdata)
- ✕ Copaco
- ✕ Workspace 365
- ✕ Ydentic
- ✕ A&M Impact

Concurrenten Exite

Ook is er gekeken naar de concurrenten van Exite. Er is gekeken naar bedrijven, welke soortgelijke diensten aanbieden als Exite.

- ✕ Previder (Previder, 2023)
- ✕ PCI (voorheen ICT Spirit) (PCI, 2023)
- ✕ Unica ICT Solutions (Unica, 2023)
- ✕ RawWorks (Rawworks, 2023)
- ✕ Intercept (Intercept, 2023)
- ✕ InSpark (Inspark, 2023)
- ✕ Rapid Circle (Rapid Circle, 2023)

4.3 Conclusie

Vanuit de contextanalyse wordt er gekeken naar randvoorwaarden, deze randvoorwaarden worden ook wel beperkende requirements genoemd. De randvoorwaarden welke uit de interne analyse komt definiëren de kaders waarbinnen de oplossing moet passen en moeten worden ingezet in dit onderzoek. Deze randvoorwaarden zijn ontstaan vanuit gesprekken met verschillende interne stakeholders. Onderstaande tabel geeft een overzicht van de opgestelde randvoorwaarden:

Nr.	Beschrijving randvoorwaarde
R01	De oplossing moet gebaseerd zijn op Microsoft technologie.
R02	Beveiliging moet voldoen aan de baselines van Exite met betrekking tot device security
R03	Omgevingen welke te veel afhankelijk zijn van on-premise infrastructuur, worden niet gemigreerd.
R04	De oplossing moet gebaseerd zijn op producten en diensten welke momenteel al geleverd worden door Exite.

Tabel 6 – Randvoorwaarden

5 Behoefteanalyse

Om de eisen en wensen van de stakeholders in kaart te brengen is er een behoefteanalyse opgesteld. Hiervoor zijn verschillende methodieken gebruikt en de resultaten daarvan worden weergegeven in requirements tabellen.

5.1 Methodiek

Voor het opstellen van de behoefteanalyse is gebruikt gemaakt van verschillende methodieken. Er zijn voornamelijk interviews gehouden en er zijn documenten geanalyseerd.

5.1.1 Interview

Om zoveel mogelijk informatie te verschaffen zijn er interviews gehouden met verschillende stakeholders. Een samenvatting van deze interviews is te vinden in bijlage B – Interviews. De stakeholders zijn in kaart gebracht door middel van het uitvoeren van een stakeholderanalyse, welke te vinden is in bijlage A – Stakeholderanalyse. De eisen en wensen zijn in kaart gebracht door de interne stakeholders te interviewen, deze zijn nauw betrokken bij het project.

5.1.2 Document analyse

Als laatste is er gekeken naar de standaard baselines van Exite. Hierin staan verschillende standaarden benoemd, welke nageleefd worden wanneer een omgeving wordt ingericht. Deze documenten zijn bekeken, omdat gedurende de interviews duidelijk is geworden dat deze aanwezig zijn en van belang kunnen zijn. Het geeft een goed beeld over welke eisen Exite stelt.

5.2 Resultaten

In onderstaande kopjes worden de tabellen weergegeven met daarin de opgestelde requirements. Een beschrijving van de kolommen is te vinden in bijlage C – Behoefteanalyse.

5.2.1 Business requirements

Nr.	Beschrijving	F/NF	Prioriteit	Genereert	Realiseert
B01	Exite zal worden voorzien van een advies om complexe on-premise omgevingen, welke in een private cloud staan, te migreren naar de public en/of hybride cloud.	F	Must	U03, U04	
B02	Exite zal worden voorzien van een ontwerp om complexe on-premise omgevingen, welke in een private cloud staan, te migreren naar de public en/of hybride cloud.	F	Must	U01, U05, U06, U07	

B03	Exite zal de oplossing bij meerdere klanten met complexe on-premise omgevingen, welke in een private cloud staan, kunnen inzetten.	F	Should	U01	
B04	De oplossing moet passen binnen het budget van de klant.	NF	Must	U03, U04	
B05	Het belang van migratie naar een digitale werkomgeving moet duidelijk zijn voor de gehele organisatie.	NF	Must	U08	

Tabel 7 – Business requirements

5.2.2 User requirements

Nr.	Beschrijving	F/NF	Prioriteit	Genereert	Realiseert
U01	De solution architecten zullen het ontwerp bij verschillende klanten met complexe on-premise omgevingen, welke in een private cloud staan, kunnen implementeren.	F	Should	S01, S03, S05, S06, S07, S08, S09, S10	B03
U02	De beheerders moeten de oplossing kunnen beheren, door wijzigingen uit te kunnen voeren.	F	Must	S01, S02, S06, S09, S10	B03
U03	De solution architecten moeten een advies krijgen hoe de on-premise omgeving, welke in een private cloud staat, gemigreerd kan worden naar de public en/of hybride cloud.	NF	Must	S01, S03, S05, S06, S07, S08, S09, S10	B01
U04	De solution architecten moeten een advies krijgen of de huidige omgeving van de klant te migreren is naar een public en/of hybride cloudomgeving.	NF	Must	S05, S08	B01
U05	De solution architecten moeten een ontwerp krijgen, waarin de huidige situatie en de nieuwe situatie wordt beschreven.	F	Must	S01, S02, S04, S05, S06, S07, S08, S09, S10	B02
U06	De solution architecten moeten een overzicht krijgen van de verbeteringen van de gewenste situatie ten opzichte van de huidige situatie.	NF	Must	S01, S02, S04, S05, S06, S07, S08, S09, S10	B02
U07	De solution architecten moeten een ontwerp krijgen, waarin het huidige	F	Should	S01, S02, S04, S05, S06, S07,	B02

	applicatielandschap in kaart gebracht wordt.			S08, S09, S10	
U08	Voor het succes van een cloudmigratie is het essentieel dat de eindgebruikers vanaf het begin betrokken zijn bij de oplossing.	NF			B04

Tabel 8 - User requirements

5.2.3 System requirements

Nr.	Beschrijving	F/NF	Prioriteit	Genereert	Realiseert
S01	De oplossing moet schaalbaar zijn, om in de toekomst gemakkelijk op en/of af te kunnen schalen in geval van veranderende behoeftes.	F	Must		U01, U02, U03, U05, U07, U08
S02	Microsoft Endpoint Manager moet zodanig ingericht worden, dat het aan de door Exite gestelde beveiligingseisen voldoet.	F	Must		U02, U05, U06, U07
S03	De oplossing moet rekening kunnen houden met on-premise infrastructuur, welke niet geschikt is voor de public en/of hybride cloud.	F	Must		U01, U03
S04	De oplossing moet samenwerken in documenten mogelijk maken voor eindgebruikers.	F	Must		U05, U06, U07
S05	De werkplek voor eindgebruikers moet flexibel zijn om niet afhankelijk te zijn van lokale infrastructuur.	F	Must		U01, U03, U04, U05, U06, U07
S06	De oplossing moet uitgebreide beveiligingsmaatregelen hebben om de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens te waarborgen.	F	Must		U01, U02, U03, U05, U06, U07
S07	De oplossing moet een infrastructuur bieden met meerdere geografische locaties en failover-mogelijkheden om een hoge beschikbaarheid van applicaties, servers en gegevens te garanderen.	F	Must		U01, U03, U05, U06, U07
S08	De oplossing moet ondersteuning bieden voor verschillende besturingssystemen.	F	Should		U01, U03, U04, U05, U06, U07

S09	De oplossing moet monitoringmogelijkheden bieden, zoals het bijhouden van prestaties, het bewaken van het gebruik van resources, het genereren van logboeken en het bieden van waarschuwingen en rapportages.	F	Must		U01, U02, U03, U05, U06, U07
S10	De oplossing moet mogelijkheden bieden voor het beheer van gegevens, zoals automatische back-ups, replicatie van gegevens naar verschillende locaties en opties voor gegevensherstel in geval van incidenten.	F	Must		U01, U02, U03, U05, U06, U07
S11	De servers welke nog draaien op Windows Server 2012 R2 moeten uitgefasseerd of vervangen worden.	F	Must		U05, U06
S12	De huidige serveromgeving dient gereduceerd te worden, zodat hierop kosten bespaard kunnen worden.	F	Must		U05, U06
S13	Het is gewenst om de servers (of een deel hiervan) te migreren naar Azure, zodat deze servers aan- en uitgezet kunnen worden, op basis van pay per use.	F	Should		U03, U04, U05, U06

Tabel 9 – System requirements

5.3 Conclusie

Op basis van de opgestelde requirements kan worden geconcludeerd dat eerst de huidige omgeving en manier van werken in kaart gebracht moet worden. Om dit te bereiken, is het nodig om de beschikbare informatie te verzamelen en te analyseren, met het oog op de huidige omgeving en manier van werken. Door deze analyse wordt inzicht verkregen op welke wijze de huidige omgeving geoptimaliseerd en gemigreerd kan worden. Dit zal inzichtelijk gemaakt worden aan de hand van een ontwerp. Het uiteindelijke advies dat voortkomt uit deze analyse en het ontwerp zal de opdrachtgever helpen bij het nemen van een beslissing over de mogelijkheid om de huidige omgeving te kunnen optimaliseren en migreren naar een public en/of hybride cloudoplossing.

6 Literatuuronderzoek

In dit hoofdstuk is literatuuronderzoek uitgevoerd om de opgestelde deelvragen te kunnen beantwoorden. Op basis van de resultaten hiervan zal een ontwerp gemaakt worden en een bijbehorend advies aan Exite.

6.1 Methodiek

Voor het uitvoeren van literatuuronderzoek is gebruik gemaakt van de methodieken deskresearch en interviews.

6.1.1 Deskresearch

Met behulp van deskresearch is er zoveel mogelijk informatie verzameld om de deelvragen te kunnen beantwoorden.

6.1.2 Interview

Met behulp van gesprekken met stakeholders is er informatie verzameld om het beantwoorden van de deelvragen te ondersteunen.

6.2 Resultaten

6.2.1 Wat is de definitie van cloudcomputing?

Volgens (Microsoft, 2023) is cloudcomputing het leveren van computingservices, inclusief servers, opslag, databases, netwerkfuncties, software, analysefuncties en intelligentie, via internet ('de cloud') waarmee snellere innovatie, flexibele resources en schaalvoordelen beschikbaar is. Doorgaans wordt er alleen betaald voor de cloudservices die gebruikt worden, waardoor er minder bedrijfskosten zijn, infrastructuur efficiënter draait en kunt schalen al naar gelang het bedrijf wijzigingen nodig heeft.

Cloudcomputing brengt een aantal belangrijke voordelen met zich mee. Er zijn zeven algemene redenen waarom organisaties cloudcomputing gaan gebruiken.

Kosten

Cloudcomputing elimineert de noodzaak om kosten te maken voor de aanschaf van hardware en software en voor het opzetten en beheren van eigen on-site datacenters (rekken met servers, de elektriciteit die dag en nacht nodig is voor stroomvoorziening en koeling, en de IT-experts die de infrastructuur moeten beheren). Dat loopt snel in de papieren.

Wereldwijde schaalbaarheid

Een van de voordelen van cloudcomputingservices is de mogelijkheid tot flexibele schaalaanpassing. In cloudtermen gesproken, houdt dat in dat het juiste aantal IT-bronnen wordt geleverd (bijvoorbeeld meer of minder rekenkracht, opslag, bandbreedte) afgesteld op de behoefte van dat moment en vanaf de juiste geografische locatie.

Prestaties

De omvangrijkste cloudcomputingservices worden op een wereldwijd netwerk van beveiligde datacenters uitgevoerd. Ze worden regelmatig bijgewerkt naar de laatste nieuwe generatie, snelle en efficiënte computinghardware. Dit heeft diverse voordelen in vergelijking met de noodzaak tot het hebben van een enkel bedrijfsdatacenter, waaronder een verminderde netwerklatentie voor toepassingen en grotere schaalvoordelen.

Beveiliging

Veel cloudproviders bieden een uitgebreide serie beleidsregels, technologieën en regelingen die de algehele beveiligingspostuur versterken. Zo worden gegevens, apps en infrastructuur beschermd tegen potentiële bedreigingen.

Snelheid

De meeste cloudcomputingservices worden als self-service op aanvraag geleverd. Daardoor kunnen zelfs grote aantallen computerbronnen in enkele minuten worden ingericht, en meestal kan dat via een paar muisklikken. Dit alles biedt bedrijven veel flexibiliteit en zorgt voor minder druk tijdens het plannen van capaciteit.

Productiviteit

On-site datacenters vereisen veel rekken en veel gestapel, hardware die moet worden ingesteld, softwarepatches die moeten worden geïnstalleerd en andere tijdrovende taken die met het beheer van IT zijn gemoeid. Cloudcomputing maakt veel van deze taken overbodig, zodat IT-teams hun tijd kunnen besteden aan het bereiken van belangrijkere bedrijfsdoelstellingen.

Betrouwbaarheid

Cloudcomputing maakt zaken als het maken van back-ups van gegevens, noodherstel na een ramp en het waarborgen van de bedrijfscontinuïteit eenvoudiger en goedkoper, omdat gegevens gespiegeld kunnen worden op meerdere redundante sites in het netwerk van de cloudprovider.

6.2.2 Wat zijn de mogelijkheden met betrekking tot een migratie naar de cloud?

Een migratie naar de cloud biedt verschillende mogelijkheden voor bedrijven en organisaties. Niet alle cloudoplossingen zijn gelijk en er bestaat geen enkel type cloudcomputing dat geschikt is voor iedereen. Er zijn verschillende modellen, typen en services ontwikkeld om je de juiste oplossing te bieden voor je behoeften.

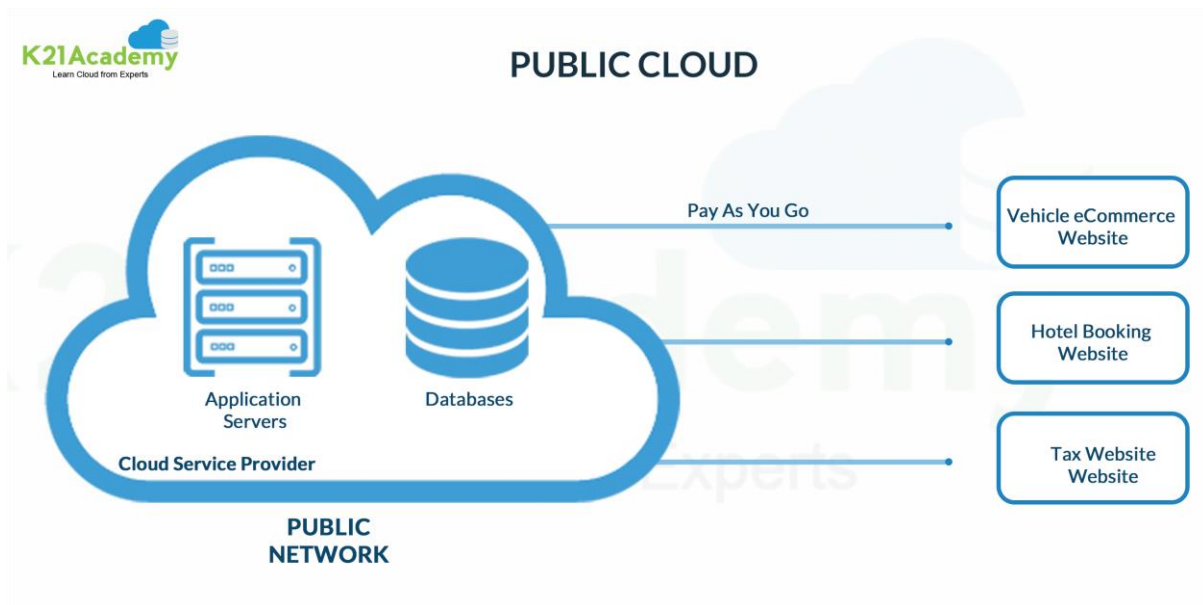
Eerst moet het type cloudimplementatie of cloudcomputingarchitectuur bepaald worden waarop je cloudservices worden geïmplementeerd. Er zijn drie verschillende manieren om cloudservices te implementeren: in een public cloud, private cloud of hybride cloud. De definities en voordelen worden in de volgende kopjes benoemd. (Microsoft, 2023)

Public cloud

Public clouds worden het meest geïmplementeerd. De cloudresources (zoals servers en opslag) zijn eigendom van en worden beheerd door een externe cloudserviceprovider. Ze worden via het internet geleverd. Bij een public cloud is alle hardware, software en andere ondersteunende

infrastructuur het eigendom van de cloudprovider en voert deze partij ook het onderhoud ervan uit. Microsoft Azure is een voorbeeld van een public cloud.

In een public cloud is het mogelijk hardware, opslag en netwerkapparaten te delen met andere organisaties of cloudtenants. De services worden benaderd en beheert middels een account op een webbrowser. Public clouds worden vaak geïmplementeerd voor webmail, online kantoortoepassingen, opslag en test- en ontwikkelomgevingen. In figuur 2 is te zien hoe een public cloud omgeving eruit kan zien:



Figuur 2 – Public cloud

Voordelen van een public cloud:

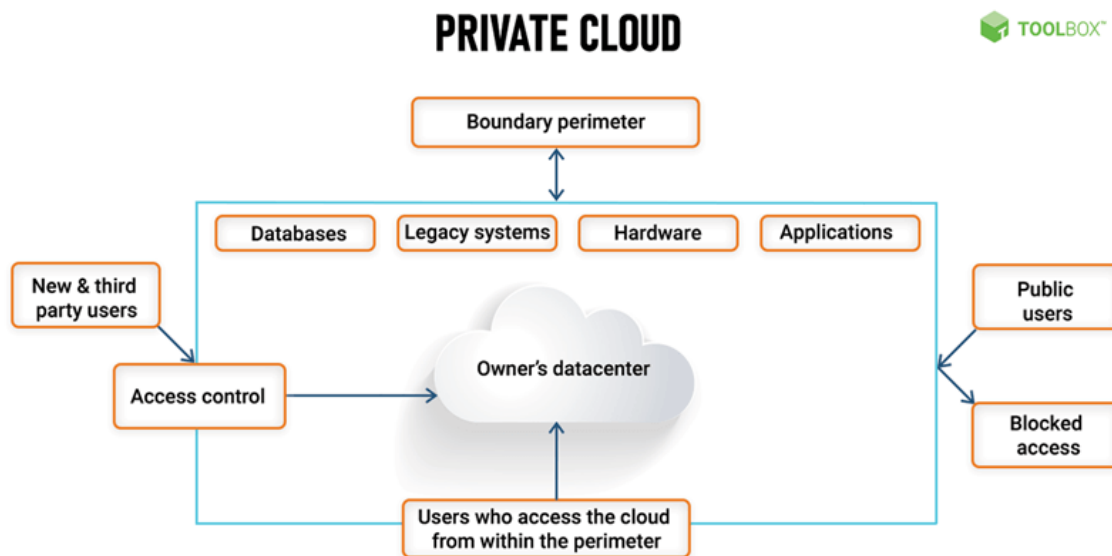
- ✗ Lagere kosten: het is niet nodig om hardware of software aan te schaffen en betaalt alleen voor de service die worden gebruikt
- ✗ Geen onderhoud: de serviceprovider zorgt voor het onderhoud
- ✗ Bijna onbeperkte schaalbaarheid: er zijn op aanvraag resources beschikbaar om aan de zakelijke behoeften te voldoen
- ✗ Hoge betrouwbaarheid: een groot netwerk van servers zorgt ervoor dat er geen storingen optreden

Private cloud

Een private cloud beschikt over resources voor cloud-computing die uitsluitend door één bedrijf of één organisatie worden gebruikt. De private cloud kan zich fysiek in het lokale datacenter van de organisatie bevinden of worden gehost door een onafhankelijke serviceprovider. In een private cloud worden de services en infrastructuur echter altijd onderhouden op een private netwerk en zijn de hardware en software uitsluitend bestemd voor de desbetreffende organisatie.

Op deze manier kan een private cloud het voor een organisatie eenvoudiger maken om de resources aan bepaalde IT-behoeften aan te passen. Private clouds worden vaak gebruikt door

overheidsinstellingen, financiële instellingen en andere middelgrote en grote organisaties met bedrijfskritieke activiteiten die meer controle over hun omgeving willen. In figuur 3 is te zien hoe een private cloud omgeving eruit kan zien:



Figuur 3 – Private cloud

Voordelen van een private cloud:

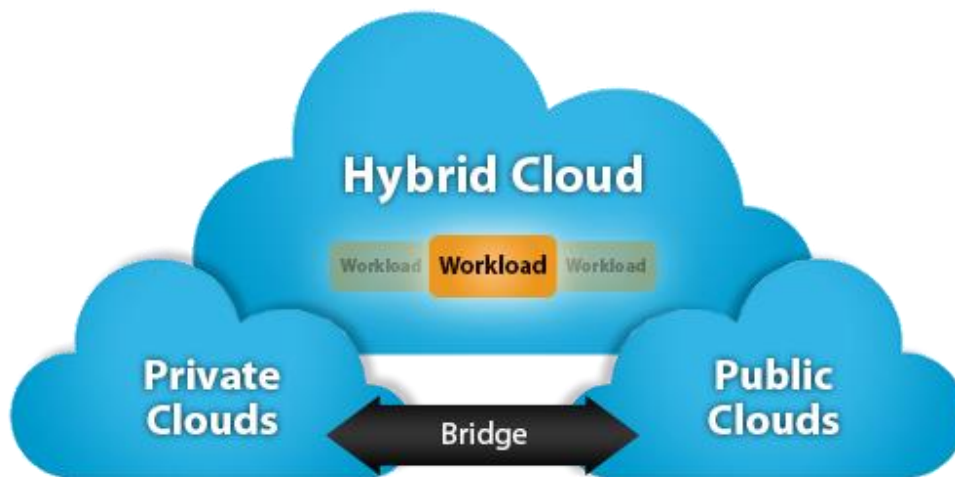
- ✗ Meer flexibiliteit: uw organisatie kan de cloudomgeving aanpassen om aan bepaalde zakelijke behoeften te voldoen
- ✗ Meer controle: resources worden niet met anderen gedeeld, dus beschik je over meer controle en privacy
- ✗ Meer schaalbaarheid: private clouds bieden vaak meer schaalbaarheid in vergelijking met on-premises infrastructuur

Hybride cloud

Een hybride cloudplatform biedt organisaties veel voordelen, zoals grotere flexibiliteit, meer implementatieopties, beveiliging, naleving en meerwaarde van de bestaande infrastructuur. Bij fluctuaties in de vraag naar rekenkracht en gegevensverwerking kan een bedrijf dankzij hybride cloud-computing de on-premises infrastructuur naadloos opschalen naar de openbare cloud voor het afhandelen van een overschot aan taken, en zonder dat externe datacenters toegang tot alle gegevens krijgen. Organisaties profiteren van de flexibiliteit en innovatie van de public cloud door bepaalde workloads uit te voeren in de cloud, waarbij uiterst gevoelige gegevens in hun eigen datacenter worden bewaard om te voldoen aan de behoeften van de client of de regelgeving.

Hierdoor kunnen bedrijven niet alleen hun computerresources opschalen, maar wordt ook de noodzaak weggenomen om grote investeringen te doen voor het afhandelen van pieken in de vraag naar meer vermogen op de korte termijn of als het bedrijf lokale resources moet vrijmaken voor meer gevoelige gegevens of toepassingen. Bedrijven hoeven alleen maar te betalen voor resources die ze tijdelijk gebruiken. Het aanschaffen, programmeren en onderhouden van extra resources en

apparatuur, die vaak langere tijd inactief zijn, is niet langer nodig. In figuur 4 is te zien hoe een hybride cloud omgeving eruit kan zien.



Figuur 4 - Hybride cloud

Voordelen van de hybride cloud:

- ✗ Controle: de organisatie kan een privé-infrastructuur gebruiken voor gevoelige bedrijfsmiddelen of workloads die lage latentie vereisen
- ✗ Flexibiliteit: het is mogelijk desgewenst te profiteren van extra resources in de public cloud
- ✗ Kosteneffectiviteit: je heb de mogelijkheid om naar de public cloud te schalen, waardoor u alleen voor extra computingvermogen betaalt wanneer dit nodig is
- ✗ Gebruiksgemak: de overstap naar de cloud hoeft niet ingewikkeld te zijn. Je kunt namelijk geleidelijk migreren en werklasten gefaseerd implementeren

6.2.3 Cloudmigratiestrategieën

Een cloudmigratiestrategie is een plan dat een organisatie hanteert om haar bestaande infrastructuur, waaronder data, applicaties, services en andere bronnen, over te brengen naar de cloud.

Het formuleren van een solide strategie is de eerste stap in het migratieproces. Het doel is om de workloads naadloos over te zetten van on-premises naar de gewenste cloudinfrastructuur, zonder dat dit invloed heeft op de beschikbaarheid of dagelijkse activiteiten.

Elke organisatie heeft echter een unieke reis naar de cloud, omdat er geen one-size-fits-all migratieplan bestaat. Elk IT-onderdeel dat gemigreerd moet worden, is uniek qua kosten, prestaties en complexiteit. Daarom kan niet elk component op dezelfde manier naar de cloud worden verplaatst. Bovendien zijn sommige workloads mogelijk niet geschikt voor migratie.

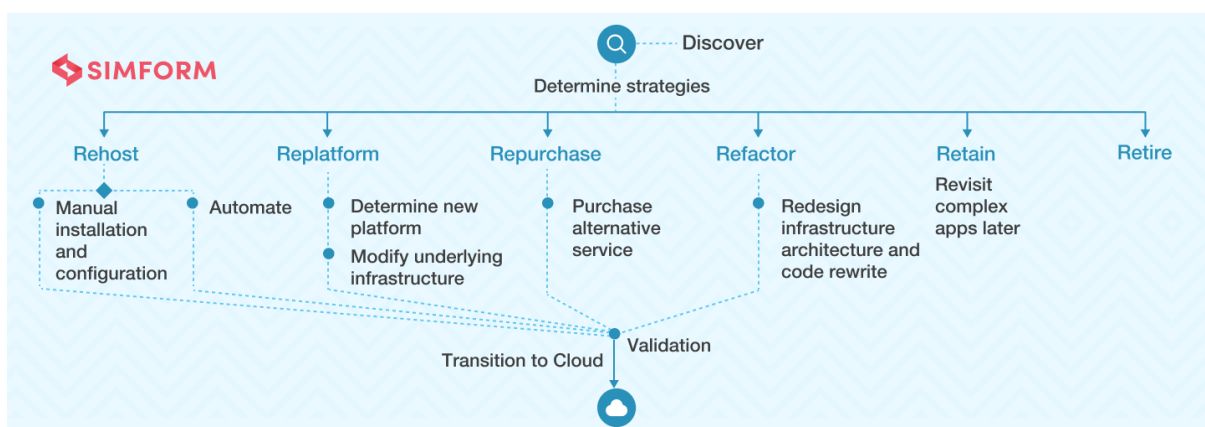
Het opstellen van een gedetailleerd migratieplan helpt bij het beantwoorden van vragen over wat, hoe en in welke volgorde deze componenten moeten worden verplaatst. Hier komen cloudmigratiestrategieën van pas. (Kotecha, 2022)

6R strategie

De 6R strategie is de meest bekende cloudmigratiestrategie. Het gebruiken van deze strategie zorgt voor enkele voordelen bij een migratie naar de cloud:

- ✕ Kosten- en tijdsbesparing
- ✕ Minder downtime en risico's
- ✕ Verbeterde schaalbaarheid
- ✕ Verbeterd de beveiliging en naleving
- ✕ Beter begrip van zaken

In figuur 5 zijn de 6R's van de cloudmigratiestrategie weergegeven. (Kotecha, 2022)



Figuur 5 – 6R strategie

Lift & Shift

Door middel van een interview met de solution architect is er uitvraag gedaan naar de mogelijkheden voor het migreren naar de cloud. De solution architect is verantwoordelijk voor het in kaart brengen van de huidige omgevingen en het ontwerpen en adviseren van een nieuwe omgeving.

De solution architect geeft aan dat lift & shift, wat een voorbeeld is van rehost in de 6R cloudmigratiestrategie, behoort tot een van de mogelijkheden. Dit houdt in dat je het huidige serverlandschap (of een deel daarvan) gaat verplaatsen van bijvoorbeeld een private cloud omgeving naar Azure public cloud. (Architect, 2023)

De lift & shift migratiestrategie een methode met de minste weerstand en is in staat de bestaande workload opnieuw te hosten zonder wijzigingen in de bestaande toepassing of een nieuw ontwerp voor hoe deze wordt gehost. (Gordon, 2021)

6.2.4 Wat moet er gedaan worden om ervoor te zorgen dat de beveiliging in de cloud voldoende is?

Om de cloud omgeving goed te kunnen beveiligen en veilig te houden zijn er een aantal zaken waar rekening mee gehouden moet worden. Door Lucidchart zijn een aantal best practices benoemd voor een veilige cloudopslag, welke in de volgende kopjes worden toegelicht. (Lucidchart, 2023)

Ken en visualiseer de gegevens

Een effectief beleid voor cloudbeveiliging begint met het begrijpen en inzichtelijk maken van de gegevens. Als je niet weet hoe een cloudprovider jouw gegevens opslaat en beheert, is het moeilijk om een beleid te implementeren dat geschikt is voor jouw bedrijf. Om een veilige cloudopslagprovider te kiezen, moet je rekening houden met de volgende vier componenten:

- ✗ Databeveiliging: dit omvat de systemen die worden gebruikt om je gegevens te beschermen
- ✗ Datalocatie: waar de servers van de cloudprovider zich bevinden, waar je gebruikers werken en hoe gegevens worden overgedragen, bepalen welke wet- en regelgeving inzake gegevensbescherming van toepassing zijn
- ✗ Datatoezicht: dit omvat hoe je gegevens worden gecontroleerd, inclusief inbraakdetectie, beveiligingsaudits en rapporten
- ✗ Databeheer: welke werknemers en opdrachtnemers van de cloudprovider hebben toegang tot jouw gegevens?

Zodra je een duidelijk beeld hebt van waar je gegevens worden opgeslagen en hoe ze worden gecontroleerd, beheerd en beschermd, kun je deze informatie vastleggen door de technische systemen te visualiseren.

Kies de juiste cloudprovider

Als je een cloudprovider kiest die strikte beveiligingsnormen hanteert, dan geef je een deel van de verantwoordelijkheid voor het beveiligen van de cloud uit handen, inclusief de naleving van wet- en regelgeving op het gebied van gegevensbescherming. Het is belangrijk om recensies van verschillende providers te onderzoeken en te kijken welke functies hen onderscheiden. Verder is het raadzaam om te kijken naar wat betrouwbare adviseurs in de sector te zeggen hebben.

Het is belangrijk om te beseffen dat er geen enkele cloudprovider is die geschikt is voor alle soorten organisaties. Je moet een provider vinden die het beste past bij jouw specifieke behoeften.

Houd rekening met wettelijke eisen

Wanneer er eenmaal een aantal cloudproviders zijn gevonden welke mogelijk geschikt zijn voor het bedrijf, dient er ook nagedacht te worden over de wettelijke vereisten voor de branche, gebruikers en landen waar het bedrijf mee te maken heeft. De cloudprovider moet uiteindelijk voldoen aan dezelfde beveiligingsvoorschriften als het bedrijf.

Versleuteling op bestandsniveau

Door gegevens op bestandsniveau te versleutelen, worden bestanden onleesbaar voor onbevoegden, met welk apparaat het bestand ook geopend wordt. Bestanden en bestandssystemen dienen versleuteld te worden voordat ze naar de cloud worden geüpload.

Beveilig apparaten van eindgebruikers

Volgens Jeff Hancock wordt 85% van de datalekken veroorzaakt door menselijke fouten. Dat houdt in dat zelfs wanneer een cloudprovider de beste beveiligingsfuncties aanbiedt, bedrijfsgegevens nog steeds een risico kunnen vormen wanneer er geen duidelijk beveiligingsbeleid is voor de eindgebruikers.

Het is belangrijk om duidelijke regels en beleidslijnen op te stellen voor wie toegang heeft tot gegevens, waarvandaan en hoe de toegang tot deze gegevens gecontroleerd wordt. Deze regels gelden voor iedereen binnen het bedrijf. Wanneer het beleid is opgesteld is het noodzakelijk dit te communiceren aan de teamleden. (Hancock, 2023)

Gebruik best practices voor wachtwoorden

Om gegevens in de cloud goed te beveiligen is het afdwingen van sterke wachtwoorden in het gehele bedrijf een belangrijke stap. Hiervoor heeft (NIST, 2021) onderstaande richtlijnen opgesteld:

- ✗ Tussen 8-64 tekens lang
- ✗ Spaties en ASCII-tekens toestaan
- ✗ Niet op de lijst met vaak gebruikte en gecompromitteerde wachtwoorden

Veel gecompromitteerde wachtwoorden zijn:

- ✗ Woordenboekwoorden
- ✗ Eerder gelekte wachtwoorden
- ✗ Herhaalde of opeenvolgende tekens
- ✗ Context specifieke wachtwoorden, zoals gebruikersnamen, bedrijfsnamen etc.

NIST raadt ook het gebruik van wachtwoordbeheertools aan.

Gebruik twee-factorverificatie

Twee-factorverificatie zorgt voor een betere beveiliging door twee vormen van verificatie te vragen, voordat een gebruiker toegang krijgt tot gegevens. De twee meest voorkomende vormen zijn:

- ✗ Iets wat je weet
- ✗ Iets wat je hebt of iets wat je bent

Iets wat je weet is het wachtwoord. Dit is de eerste stap. Nadat het wachtwoord is ingevoerd, komt de volgende stap in de vorm van iets wat je hebt (code die naar een apparaat verstuurd wordt) of iets wat je bent (vingerafdruk of gezichtsscan). Op deze manier is de toegang tot (kritieke) gegevens veel veiliger.

Veilige gegevens overdracht

Gegevens die in de cloud zijn opgeslagen moeten niet alleen beveiligd worden wanneer ze zijn opgeslagen, maar ook wanneer ze worden overgedragen. Door bijvoorbeeld versleuteling, SSL en veilige e-mailapplicaties te gebruiken.

Maak back-ups van gegevens

Als laatste is het verstandig om geregeld een back-up te maken en deze op te slaan op meerdere verschillende locaties. Zo voorkom je het risico van gegevensverlies in het geval van een beveiligingslek of een aanval.

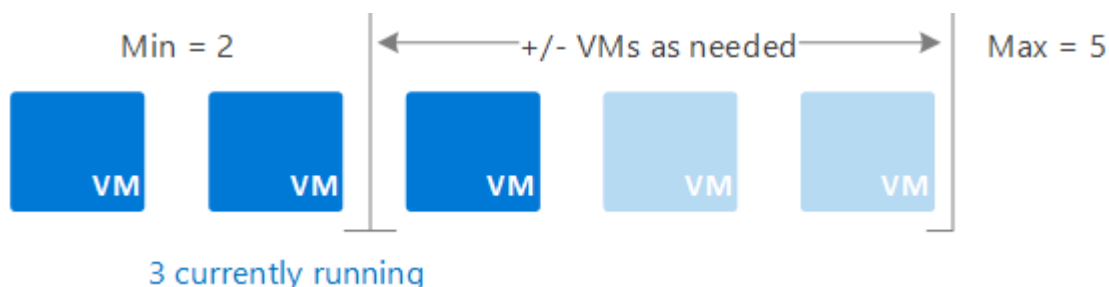
Het is wel van belang dat de beveiligingsnormen op een secundaire locatie minstens net zo streng zijn als op de primaire locatie. Zo lopen de back-up gegevens geen extra beveiligingsrisico's.

6.2.5 Hoe kan een cloudoplossing schaalbaar worden gemaakt?

Schaalbaarheid is een systeem dat snelle veranderingen in werklust en vraag kan verwerken. De schaalbaarheid geeft aan hoe goed dat systeem reageert op veranderingen door resources toe te voegen of te verwijderen om aan de vraag te voldoen. De architectuur is het geheel van hardware, software, technologie en best practices waarop de netwerken, toepassingen, processen en services in je hele systeem steunen. (Lucidchart, 2023)

Automatisch schalen

Met automatisch schalen is het mogelijk om moeiteloos de juiste hoeveelheid resources toe te wijzen om de belasting van een applicatie te kunnen verwerken. Automatisch schalen voegt resources toe of schakelt deze juist af om piekbelastingen, zoals seizoensgebonden workloads, effectief aan te kunnen. Daarnaast worden niet-actieve resources uitgeschakeld of wordt de capaciteit verminderd om kosten te besparen tijdens periodes van verminderde belasting, zoals 's nachts en in het weekend voor bepaalde bedrijfsapplicaties. Met automatisch schalen worden de aantallen virtuele machines (VM's) automatisch aangepast binnen een vooraf ingesteld minimum- en maximumbereik, waarbij VM's automatisch worden toegevoegd of verwijderd op basis van specifieke regels. (Microsoft, 2023)



Figuur 6 - Automatisch schalen

Automatisch schalen kan ook ingezet worden voor Citrix omgevingen. Automatisch schalen is een functie die exclusief beschikbaar is in Citrix DaaS (voorheen Citrix Virtual Apps and Desktops-service) en zorgt voor een consistente en hoogwaardige oplossing om proactief het energiebeheer van

machines te regelen. Het heeft als doel kosten en gebruikerservaring in balans te brengen. Automatisch schalen integreert de verouderde Smart Scale-technologie in de oplossing voor energiebeheer van de Manage-console. (Shanmugiah, 2022)

Automatisch schalen wordt ondersteund door de volgende public cloud platformen:

- ✕ Microsoft Azure (resource manager)
- ✕ Amazon Web Services
- ✕ Google Cloud Platform

Horizontaal en verticaal schalen

Er zijn twee manieren waarop een applicatie geschaald kan worden: verticaal schalen en horizontaal schalen. Bij verticaal schalen, ook wel upscaling genoemd, wordt de capaciteit van een resource vergroot, bijvoorbeeld door gebruik te maken van een grotere VM. Bij horizontaal schalen, ook wel outscaling genoemd, worden er nieuwe instanties van een resource toegevoegd, zoals VM's of database-replica's.

Een voordeel van verticaal schalen is dat het mogelijk is om de capaciteit te vergroten zonder de applicatie zelf aan te passen. Echter, er komt een punt waarop verticaal schalen niet langer mogelijk is. Op dat moment moet er overgestapt worden op horizontaal schalen.

Horizontaal schalen biedt belangrijke voordelen ten opzichte van verticaal schalen:

- ✕ Echte cloudschaal: Applicaties kunnen ontworpen worden om te draaien op honderden of zelfs duizenden nodes, waardoor schaalaanpassingen mogelijk zijn die niet haalbaar zijn op één enkel knooppunt
- ✕ Elasticiteit: Horizontaal schalen maakt het mogelijk om meer instanties toe te voegen wanneer de belasting toeneemt, en instanties te verwijderen tijdens rustigere perioden. Dit zorgt voor flexibiliteit en efficiënt resourcegebruik
- ✕ Automatische schaling: Horizontaal schalen kan automatisch geactiveerd worden op basis van een planning of als reactie op veranderingen in de belasting
- ✕ Kostenbesparing: Horizontaal schalen kan kosteneffectiever zijn dan verticaal schalen, omdat het uitvoeren van meerdere kleine VM's vaak minder kost dan het uitvoeren van één grote VM
- ✕ Verbeterde betrouwbaarheid: Horizontaal schalen kan de betrouwbaarheid vergroten door redundantie toe te voegen. Als een instantie uitvalt, blijft de applicatie actief dankzij de beschikbare instanties

Kortom, horizontaal schalen biedt flexibiliteit, kostenefficiëntie en betrouwbaarheid, waardoor het een krachtige benadering is voor het schalen van applicaties in de cloud. (Microsoft, 2023)

6.2.6 Welke gevolgen zou een migratie naar de cloud met zich mee brengen voor de klant?

Cloudmigraties hebben altijd gevolgen op voornamelijk de eindgebruikers, omdat zij er immers mee moeten kunnen werken. Volgens de customer success manager is het belangrijk om eindgebruikers (key users) mee te nemen in de gehele verandering/migratie. Dat wordt ook wel de adoptie genoemd. Om dat goed te kunnen faciliteren wordt er altijd een pilotfase opgezet om de veranderingen te testen. In de fase daarna komt de livegang/daadwerkelijke migratie met bijbehorende nazorg. (Success Manager, 2023)

Onvoorspelbare kosten

Op dit moment omarmen veel organisaties de cloud zonder zorgvuldig na te denken over de voordelen die de cloud zou moeten bieden en welke essentiële aspecten daarvoor op orde moeten zijn. Het gebrek aan grondige overweging leidt tot onvoorspelbare kosten en een aanzienlijk risico op een teleurstellende cloud-implementatie die niet aan de verwachtingen voldoet.

Bovendien is het tijdstip waarop je overstapt naar de cloud ook van invloed. Een verstandig moment hiervoor is bijvoorbeeld wanneer je bedrijf aanzienlijke groei doormaakt en behoefte heeft aan schaalbare diensten. Ook wanneer je kiest voor innovatieve diensten die gebruikmaken van complexe technologieën zoals kunstmatige intelligentie, is het moment van overstappen relevant. Hetzelfde geldt wanneer je gedwongen wordt om een keuze te maken voor nieuwe hardware, wat meestal eens in de drie tot vijf jaar voorkomt.

Kritische benadering

Een kritische benadering is essentieel voor een succesvolle overgang van applicaties en infrastructuur naar de cloud. Hierbij is het belangrijk om je af te vragen of alle systemen moeten worden gemigreerd naar de cloud, of dat bepaalde systemen, zoals een kostbare telefooncentrale, beter on-premises kunnen blijven. In het geval van applicaties die al gebreken vertonen of niet correct zijn geconfigureerd on-premises, is het verstandig om deze eerst aan te passen voordat ze worden gemigreerd naar de cloud.

Bovendien zijn er specifieke toepassingen die offline moeten blijven werken, zoals software voor het beheer van magazijnen en kassen. Het is belangrijk om deze toepassingen buiten de cloud te houden, aangezien ze niet geschikt zijn voor een online omgeving.

Kortom, een kritische evaluatie van welke systemen geschikt zijn voor de cloud en welke eerst aangepast moeten worden, evenals het identificeren van toepassingen die offline moeten blijven werken, draagt bij aan een succesvolle migratie naar de cloud.

Drie risico's

Een versnelling van de migratie naar de cloud brengt risico's met zich mee. Dit kan ten koste gaan van de kwaliteit van digitale dienstverlening en de businesscontinuïteit. Het te snel inrichten leidt tot drie belangrijke risico's:

- ✗ Een grotere kans op datalekken en cyberaanvallen, bijvoorbeeld doordat niet de juiste beveiligingsmaatregelen zijn toegepast
- ✗ Onnodig hoge kosten voor datgene wat je naar de cloud brengt, onder andere door verkeerde keuzes in clouddiensten en het niet realiseren van optimalisatie van de cloud-inrichting door het uitzetten van de testomgevingen
- ✗ Een niet stabiele cloud-omgeving als gevolg van instabiele applicaties die niet zijn aangepast naar de cloudschaal. Denk aan resiliency

"Zelfs als er een goede reden is om een migratie naar de cloud te maken en er een doortimmerd plan ligt, is er een kans dat je belangrijke aspecten over het hoofd ziet"

In de praktijk wordt vaak over belangrijke aspecten heen gekeken, zoals compliance en privacy. Het is essentieel om hier aandacht aan te besteden. Begin daarom altijd met het uitvoeren van een BIV-classificatie (Beschikbaarheid, Integriteit, Vertrouwelijkheid) van de applicatiesuite die je wilt migreren naar de cloud. Beoordeel vervolgens of de juiste maatregelen zijn genomen, zowel op het gebied van infrastructuur als applicatie, om aan deze classificatie te voldoen. (Knulst, 2022)

6.2.7 Wat zijn de huidige knelpunten op het gebied van beveiliging?

Door middel van een interview met de customer success manager zijn de huidige knelpunten uitgevraagd. Uit het interview is gebleken dat de klant momenteel twee grote knelpunten heeft. De klant heeft een legacy omgeving waar ze moeilijk van af kunnen en ze hebben een Citrix omgeving, waar ze weinig van de Microsoft 365 facetten kunnen benutten. Dit houdt in dat de omgeving erg statisch is. Ook wordt er nog deels lokaal gewerkt. Dit houdt in dat er vanuit twee omgevingen gewerkt wordt.

Data staat momenteel opgeslagen op verschillende locaties. Een gedeelte staat op Teams/SharePoint en OneDrive en een gedeelte staat op verschillende netwerkshares opgeslagen. Ook staat er veel archiefdata opgeslagen op een lokale NAS (Network Attached Storage), welke de klant zelf in beheer heeft. Op den duur is dit apparaat afgeschreven en moet er gekeken worden naar een nieuwe oplossing. Ook is deze huidige manier van archiefdata een knelpunt, omdat deze data niet redundant opgeslagen staat of wordt meegenomen in een back-up.

Vanuit het beveiligingsperspectief staat data nu op verschillende plekken en is het werkplekbeheer, wat gedaan wordt middels Microsoft Intune, niet goed ingericht en voldoet het niet aan de baseline device security van Exite. De beveiliging kan hierdoor niet 100% worden afgedicht en vormt een risico voor de klant. (Success Manager, 2023)

6.2.8 Wat zijn de kritische succesfactoren om het project te doen slagen voor een klant?

Door middel van een interview met de customer success manager, welke nauw betrokken is bij projecten voor klanten, zijn kritische succesfactoren uitgevraagd welke belangrijk zijn voor Exite. Uit het interview is gebleken dat het voor Exite belangrijk is dat er wordt begonnen met kijken naar in welke situatie de klant momenteel zit. Er moet gekeken worden naar hoe er nu gewerkt wordt (huidige situatie) en of dat aansluit bij de visie van de klant. Vanuit daar moet er gekeken worden in hoeverre Exite de klant het beste kan faciliteren. Exite geeft aan dat, wanneer je een plan opstelt wat vanaf de start van het project niet doelt op de juiste zaken, het vanaf dat punt al mis zal gaan. Wat ook erg belangrijk is, is om voortdurend na te denken over de aanpak van de adoptie, het stuk verandermanagement.

Ook is het van belang om goed in kaart te krijgen wat op welke plek staat. Het beleid moet duidelijk zijn, zodat daar ook kritisch naar gekeken kan worden en mogelijk geoptimaliseerd kan worden.

Verder is communicatie belangrijk. Klanten willen graag op de hoogte gehouden worden van de voortgang en ontwikkelingen. Zodra klanten goed meegenomen worden in de gehele migratie, zal de adoptie en daadwerkelijke livegang ook soepeler verlopen. (Success Manager, 2023)

Kritische succesfactor 1

Het belang van migratie naar een digitale werkomgeving moet duidelijk zijn voor de gehele organisatie.

In het verleden werd automatisering voornamelijk vanuit het management top-down gestuurd, waarbij een plan werd opgesteld voor de implementatie van systemen. De huidige trend is echter dat medewerkers op de werkvloer al in een vroeg stadium worden betrokken bij het opstellen van het implementatieplan. Zij hebben namelijk waardevolle kennis van de werkprocessen en weten hoe ze beter en efficiënter kunnen werken.

Het is belangrijk om te begrijpen dat elke afdeling en gebruikersgroep binnen de organisatie een andere reden heeft om naar de cloud te migreren. Voor IT-management zijn bijvoorbeeld informatiebeveiliging en systeemcontinuïteit twee belangrijke pijlers. Businessmanagers en eindgebruikers hechten veel waarde aan het verbeteren van de productiviteit. Senior management en directie kijken naar kosten, de toekomstbestendigheid van de oplossing en hoe ze met moderne technieken de processen kunnen heroverwegen of zelfs opnieuw kunnen inrichten om efficiënter te kunnen werken. (Kieft, 2022)

Kritische succesfactor 2

Een kritieke succesfactor is het begrijpen waar je vandaan komt en waar je naartoe wilt. Er is een duidelijk verschil tussen hoe vroeger werd gewerkt en hoe het nu gaat. Vroeger was alles hiërarchisch georganiseerd en werden veranderingen top-down doorgevoerd. Tegenwoordig streven organisaties veel meer naar samenwerking op een netwerkachtige manier. Multidisciplinair

samenwerken, waarbij iedereen zijn of haar kracht benut, is hierbij essentieel. Dit betekent dat bestanden en documenten door de hele organisatie, zelfs extern, worden gedeeld.

Om dit te faciliteren, is een geschikt en veilig systeem nodig. Het is belangrijk om de ambities van de organisatie te bekijken om de juiste keuze te maken. Ga op verkenning en ontdek wat medewerkers echt belangrijk vinden. Wat gebruiken ze nu al en wordt het efficiënt gebruikt? Waar wil de organisatie naartoe? Deze inzichten zijn cruciaal bij het vormgeven van de IT-inrichting. (Kieft, 2022)

Kritische succesfactor 3

Veel MKB-bedrijven hebben een interne IT-afdeling om de dagelijkse werkzaamheden te kunnen beheren. Vaak proberen ze ook specialistische taken, zoals een cloudmigratie, zelf uit te voeren om kosten te besparen.

In de praktijk blijkt dat het beter is om specialistische taken toe te vertrouwen aan partijen die de kennis, vaardigheden en tools hebben en dit als dagelijkse activiteit uitvoeren. Op deze manier kan het bedrijf gewoon doorgaan zonder dat de migratie te veel tijd en moeite van interne medewerkers vergt. De directie kan zich richten op de eindgebruikers en draagvlak creëren, terwijl de IT-afdeling zich bezighoudt met de functionele vertaling voor de eindgebruikers en de migratie op de achtergrond plaatsvindt.

Dankzij moderne technologie zijn medewerkers beter bereikbaar, kunnen ze sneller reageren en efficiënter omgaan met reistijd, wat de productiviteit ten goede komt. Bovendien zijn verouderde ICT-systemen energieslurpers binnen organisaties en kostbaar in onderhoud. Het is essentieel om de juiste processen en tools (inclusief trainingen) te bieden om dit te realiseren. (Kieft, 2022)

Kritische succesfactor 4

Voor het succes van een cloudmigratie is het essentieel dat de eindgebruikers vanaf het begin betrokken zijn bij de oplossing. Ze moeten de toegevoegde waarde van de cloudmigratie begrijpen en de uitgebreide mogelijkheden optimaal kunnen benutten.

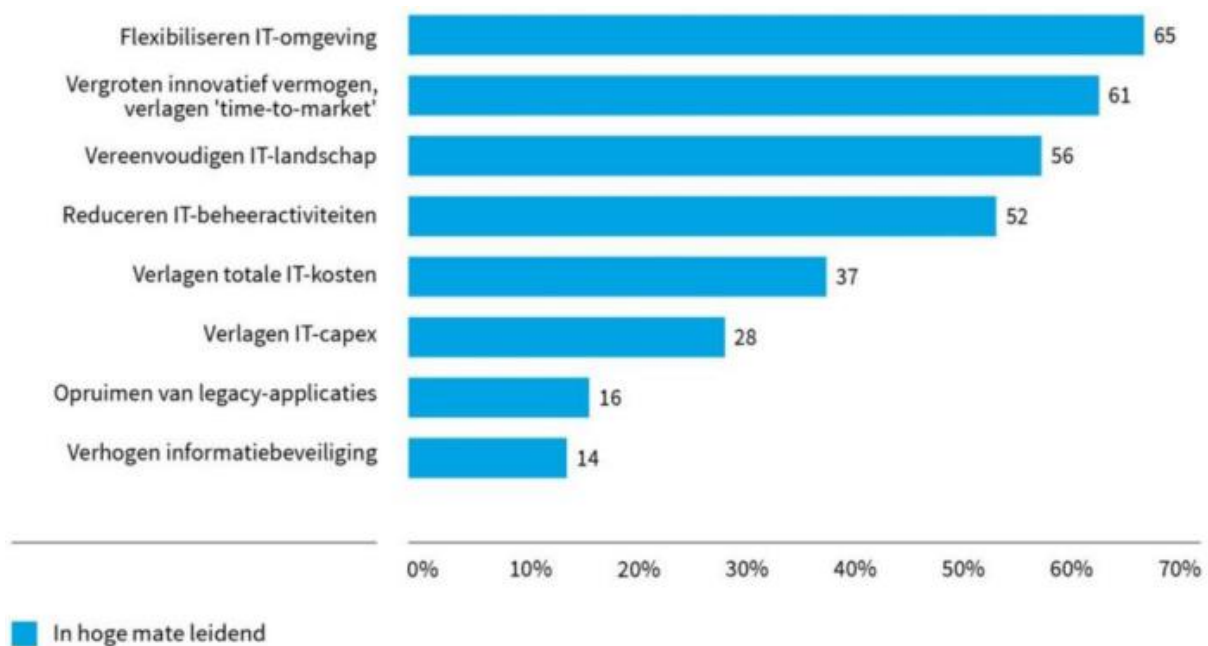
Het slagen van een cloudmigratie hangt af van de adoptie, en dit gaat verder dan alleen het geven van een training over het vinden van bepaalde applicaties vanaf het moment van implementatie. Het is een volledige verandering van de manier van werken. Als dit niet goed begeleid wordt, vallen mensen snel terug in oude gewoonten en mis je de boost in productiviteit die de cloud kan bieden. (Kieft, 2022)

Kritische succesfactor 5

Om eindgebruikers te helpen wennen aan en te leren werken via de cloud, is het belangrijk om de migratie in behapbare stappen te implementeren. Hierbij kunnen ze eerst wennen aan en leren werken met het eerste deel voordat het volgende deel wordt geïntroduceerd. Op deze manier wordt draagvlak en acceptatie gecreëerd bij de eindgebruikers.

Elke organisatie bevindt zich in een andere fase van de digitale transformatie. Met behulp van een Cloud Readiness Scan kan worden bepaald in hoeverre een organisatie gevorderd is in dit proces. Op basis van de resultaten van deze scan wordt een roadmap opgesteld om de cloudmigratie te initiëren. Hierbij wordt gestart met de onderdelen die het meest relevant zijn voor de specifieke organisatie. (Kieft, 2022)

In figuur 7 is te zien wat de acht meest voorkomende motieven zijn voor cloudmigraties.



Figuur 7 - Motieven cloudmigraties

6.2.9 Archiefdata opslag mogelijkheden

Uit de analyse is gebleken dat de desbetreffende klant gebruik maakt van een lokale NAS (Network Attached Storage). Vanuit Exite worden ook Cloud NAS oplossingen aangeboden, waaronder Wasabi Cloud NAS. In dit kopje worden de mogelijkheden van Wasabi onderzocht.

Wasabi Cloud NAS is snelle, veilige en kosteneffectieve netwerkopslag in de cloud. Het is mogelijk om te verbinden met de bestaande on-premises NAS om automatisch statische data over te zetten naar goedkope Wasabi cloud-opslag. Het kan gebruikt worden om servercapaciteit vrij te maken terwijl de gegevens beschikbaar en binnen milliseconden opvraagbaar blijven. (Wasabi, 2023)

Wasabi biedt enkele voordelen ten opzichte van een on-premise NAS:

- ✗ Altijd vrije ruimte beschikbaar: Wasabi Cloud NAS creëert een "bodemloze" opslagcapaciteit
- ✗ Behoud van huidige activiteiten: Geen nieuw bestandssysteem om te leren
- ✗ Verlagen van kapitaalkosten: Geen periodieke hardware upgrades en gedoe met gegevensmigratie meer
- ✗ Geen on-premise ruimte nodig: Neemt geen on-premise ruimte in beslag, geen elektriciteit nodig en geen menselijk onderhoud vereist

- ✕ Veel betrouwbaarder dan de meeste lokale opslag
- ✕ Bescherming tegen ransomware, door data immutable te maken (TIBCO, 2023)
- ✕ Herstel gegevens vanuit de cloud als lokale schijven falen of gegevens verloren gaan

Figuur 8 laat zien dat dat de Wasabi Cloud NAS een kostenbesparende oplossing is ten opzichte van een on-premise NAS of een dataopslag in bijvoorbeeld AWS, Microsoft Azure of Google Cloud Platform. (Wasabi, 2023)

	On Premises	Amazon S3 (Cloud 1.0)	Wasabi (Cloud 2.0)
			
Equipment costs depreciated over 5 years	\$69K	N/A	N/A
Maintenance fees ¹	\$62K	N/A	N/A
Power and networking	\$87K	N/A	N/A
Staffing and overhead	\$52K	N/A	N/A
Storage costs ²	N/A	\$289K	\$73K
Total costs	\$270K	\$289K	\$73K

¹ assuming 20% annual maintenance and support

² assuming average 20% egress download per month

Figuur 8 – Vergelijking NAS

Ook biedt Wasabi data opslag mogelijkheden in West-Europa, wat op het gebied van beveiliging een voordeel is.

6.2.10 Remote Desktop Services

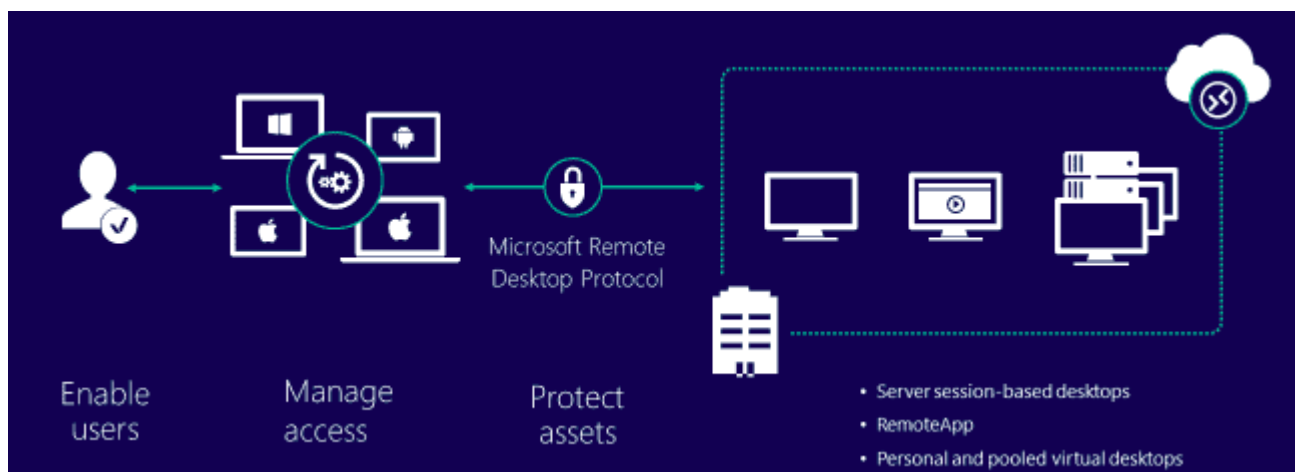
Remote Desktop Services (RDS), voorheen bekend als Terminal Services, is een set technologieën ontwikkeld door Microsoft om thin client-oplossingen te bieden.

Met RDS kunnen gebruikers verbinding maken met virtuele desktops of applicaties die worden gehost op servers. In plaats van dat de gebruiker de sessie lokaal op zijn eigen computer verwerkt, wordt deze altijd gehost en afgehandeld op de server. Dit maakt het mogelijk om met minimale systeembronnen verbinding te maken met geavanceerde rekenkracht en applicaties, zelfs vanaf eenvoudige thin clients.

Dankzij RDS kunnen gebruikers overal en altijd toegang krijgen tot hun desktopomgeving of de gewenste applicaties, zolang ze een netwerkverbinding hebben. Dit maakt het mogelijk om flexibel te werken en productief te blijven, zelfs wanneer men niet fysiek aanwezig is op het kantoor.

Met behulp van RDS kunnen organisaties de kosten verlagen en de beheerinspanning verminderen, omdat applicaties en desktopomgevingen centraal kunnen worden beheerd en bijgewerkt op de server. Dit maakt het eenvoudiger om patches en updates toe te passen, de beveiliging te handhaven en gebruikersrechten te beheren.

Al met al biedt RDS een efficiënte en flexibele manier om thin client-oplossingen aan te bieden, waardoor gebruikers toegang hebben tot virtuele desktops en gehoste applicaties zonder dat ze zware systeemvereisten nodig hebben op hun eigen computers. In figuur 9 is te zien hoe een RDS-omgeving werkt. (Jethva, 2022)



Figuur 9 – Remote Desktop Services

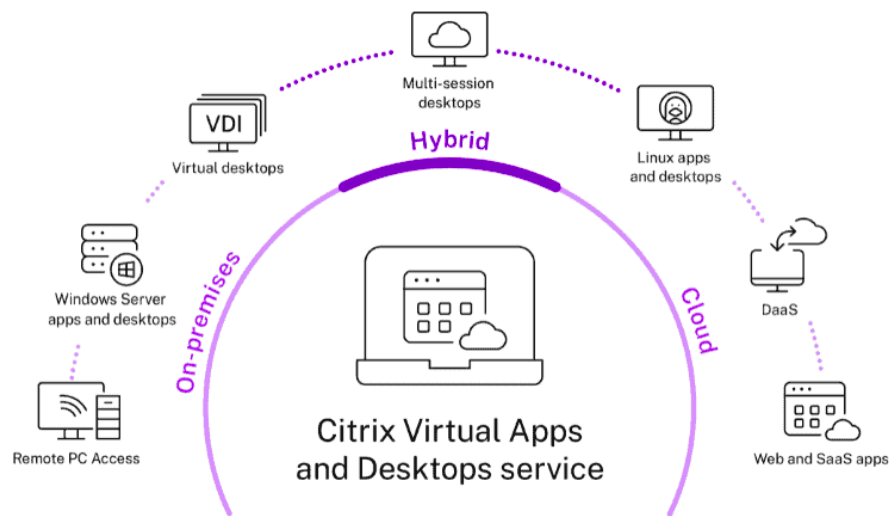
6.2.11 Citrix

Met Citrix XenDesktop kunnen gebruikers op een vergelijkbare manier als bij Microsoft RDS overal toegang krijgen tot hun desktopomgeving of software. Het onderscheidende kenmerk van Citrix is het centrale beheerplatform dat ze hebben ontwikkeld, waardoor netwerkmonitoring en schaalbaarheid eenvoudiger zijn geworden en een betere gebruikerservaring wordt gegarandeerd.

Het Citrix-beheerplatform biedt tools en functionaliteiten die het beheer van virtuele desktops en applicaties vereenvoudigen. Het stelt beheerders in staat om het netwerk te monitoren, de prestaties te optimaliseren en schaalbaarheid te realiseren zonder complexe configuraties. Dit platform verbetert ook de gebruikerservaring door snelle en betrouwbare toegang tot virtuele desktops en applicaties te bieden, ongeacht de locatie of het gebruikte apparaat.

Met Citrix kunnen organisaties profiteren van geavanceerde virtualisatietechnologieën om flexibiliteit, mobiliteit en efficiëntie te bevorderen. Het stelt gebruikers in staat om altijd toegang te hebben tot hun werkplek en applicaties, ongeacht waar ze zich bevinden. Het centrale beheerplatform zorgt voor eenvoudig beheer en schaalbaarheid, waardoor IT-teams tijd en moeite

kunnen besparen bij het implementeren en onderhouden van virtuele desktop- en applicatie-omgevingen. In figuur 10 is te zien hoe een Citrix omgeving werkt. (Jethva, 2022)



Figuur 10 – Citrix

6.3 Conclusie

Vanuit het literatuuronderzoek zijn onderstaande ontwerpprincipes opgesteld. Deze vormen de input voor het ontwerp en het advies.

Nr.	Beschrijving ontwerpprincipe
OP1	Als de oplossing schaalbaar moet zijn, moeten de resources aangepast kunnen worden op basis van veranderende behoeften.
OP2	Als de oplossing beheerd moet worden door Exite, is toegang tot de resources met admin roles benodigd.
OP3	Als samenwerken in documenten mogelijk moet zijn, moet centrale opslag van data ingericht worden.
OP4	Als werkplekken voldoende beveiligd moeten zijn, moet Microsoft Endpoint Manager ingericht worden op basis van de gestelde vereisten van Exite.
OP5	Als de beveiliging in de cloud goed ingericht moet zijn, moet er rekening gehouden worden met verschillende aspecten op basis van best practices.
OP6	Als Exite de huidige IT-omgeving wilt optimaliseren en migreren, dan moet er eerst gekeken worden naar de huidige omgeving en manier van werken.
OP7	Als de beveiliging van de data goed ingericht moet zijn, moet er automatische back-up van gegevens ingericht worden.
OP8	Als Exite een omgeving wilt optimaliseren en migreren, dan moet de omgeving zo eenvoudig mogelijk worden opgezet.

Tabel 10 – Ontwerpprincipes

7 Ontwerp

In dit hoofdstuk wordt het ontwerp beschreven hoe de huidige omgeving geoptimaliseerd en gemigreerd kan worden naar een public en/of hybride cloudoplossing.

7.1 Methodiek

Gedurende het vooronderzoek zijn in verschillende hoofdstukken requirements, randvoorwaarden en ontwerpprincipes geïdentificeerd. Dit hoofdstuk richt zich op het creëren van een ontwerp voor het optimaliseren en migreren van on-premise omgeving naar een oplossing op basis van een public en/of hybride cloudoplossing. Het ontwerp zal in hoofdstuk 9 worden geëvalueerd aan de hand van de requirements.

7.2 Vereiste functionaliteiten

Uit het onderzoek is gebleken dat wanneer Exite complexe on-premise omgevingen, welke in een private cloud draaien, wilt optimaliseren en migreren naar een public en/of hybride cloudoplossing, dat het vereist is om de huidige omgeving en manier van werken van een klant goed in kaart te brengen. Op basis daarvan kunnen de eisen en wensen van deze klant in kaart gebracht worden, zodat daar een passend maatwerk oplossing voor gemaakt kan worden welke aansluit bij de visie van de klant.

Verder is uit gesprekken met de customer succes manager gebleken dat de gehele Microsoft365 omgeving geoptimaliseerd moet zijn, zodat zoveel mogelijk facetten uit dat pakket benut kunnen worden. Het komt geregeld voor dat er momenteel weinig facetten uit het pakket gebruikt worden, terwijl daar wel voor betaald wordt in de licenties. Ook zal Microsoft Endpoint Manager (Intune) zodanig ingericht moeten worden, dat het voldoet aan de door Exite gestelde eisen.

On-premise serveromgevingen dienen gereduceerd te worden (waar mogelijk), zodat kosten bespaard kunnen worden. Uit onderzoek is gebleken dat servers uitgefasseerd kunnen worden en dat bepaalde servers niet iedere dag gebruikt worden. Dit is te zien in de huidige situatie, welke beschreven is in het volgende hoofdstuk. Hierom is het gewenst om deze servers (of een deel hiervan) te migreren naar Azure, zodat deze servers aan- en uitgezet kunnen worden, op basis van pay per use. Op deze wijze zijn on-premise serveromgevingen te downsizen. Er wordt gekozen voor Azure, omdat dit is voortgekomen uit de randvoorwaarden.

Ook is het van belang om de servers, welke nog draaien op Windows Server 2012 R2, uit te faseren of opnieuw opgezet moeten worden. Dit besturingssysteem wordt namelijk vanaf oktober 2023 niet meer ondersteund en krijgt geen beveiligingsupdates meer, wat een risico vormt voor de klant. (Microsoft, 2023)

Verder is uit het onderzoek gebleken dat het belangrijk is om gebruik te maken van best practices met betrekking tot het inrichten van beveiliging op de laptops en desktops van de eindgebruikers.

Onderstaande ontwerpprincipes komen aan bod in het ontwerp:

Functionaliteit	Ontwerpprincipe
Schaalbaarheid	OP1
Monitoring en beheer uitbesteden	OP2
Samenwerken in documenten	OP3
Inrichting Microsoft Endpoint Manager	OP4, OP5
Back-up van gegevens	OP7
Beveiliging in de cloud op basis van best practices	OP4, OP5

Tabel II – Ontwerpprincipes

7.3 Huidige situatie

In dit hoofdstuk wordt de huidige situatie in kaart gebracht. Op basis daarvan kan een nieuwe situatie geschetst worden, waarin de vereiste functionaliteiten verwerkt zijn.

Uit onderzoek en analyse is gebleken dat de IT-infrastructuur complex is ingericht. De complexe inrichting houdt in dat de omgeving veel afhankelijk is van on-premise infrastructuur. Er wordt onder andere gebruik gemaakt van een verouderde Citrix omgeving. Deze omgeving heeft een aantal servers nodig welke nog draaien op Windows Server 2012 R2. Deze omgeving wordt momenteel alleen nog gebruikt door een klein aantal gebruikers en wordt voornamelijk gebruikt voor het inzien van archiefdata (SAP) en generieke applicaties. Het aantal servers, te zien in bijlage E – Onderzoek huidige omgeving, wat hier voor benodigd is staat niet in verhouding met de hoeveelheid gebruikers. Ook wordt er gebruik gemaakt van laptops, welke middels Microsoft Endpoint Manager zijn uitgerold. Momenteel is dit erg matig en minimaal ingericht en voldoet de inrichting niet aan de beveiligingseisen van Exite. Deze beveiligingseisen zijn beschreven in hoofdstuk 7.4.1 inrichting Intune.

Alle servers staan momenteel opgenomen in de private cloud. Middels een site2site VPN verbinding worden deze servers benaderd. Op locatie bij de klant staan momenteel laptops, welke zijn opgenomen in Intune en CAD workstations. De CAD workstations zijn niet opgenomen in Intune. Ook staat op locatie een NAS, waarop veel archiefdata is opgeslagen en in beheer is door de klant zelf. De printers die ook op locatie staan worden gebruikt en beheerd middels een printserver, welke ook in de private cloud is opgenomen.

7.3.1 Verouderde servers

Uit het onderzoek in bijlage E – Onderzoek huidige situatie blijkt dat er ook andere servers aanwezig zijn welke nog draaien op Windows 2012 R2, deze servers dienen voor oktober 2023 uitgefasseerd of vervangen te zijn. Dit besturingssysteem krijgt vanaf dat moment geen ondersteuning en beveiligingsupdates meer. Onderstaande servers zullen vervangen of uitgefasseerd moeten worden voor oktober 2023:

Servernaam	Rol	CPU	RAM	HDD	Opmerking
APP01	SQL Server (SAP) / Exchange Management	4	32	350	SQL Server SAP, huidige memory gebruik 37% (20GB beschikbaar)
APP02	SQL Server (Stratech SPS) / SVN Server	2	8	100	SQL Server Stratech SPS
APP03	MySQL / OpenVPN / TCserver / GTP Tracker	4	4	140	D: schijf niet in gebruik
DC01	Domain Controller / Fileserver / DNS / DHCP / Radius server / eBridge MFP software (Toshiba)	2	8	3600	Shares worden aangeboden met DFS / actieve DHCP server / Radius tbv SonicWall NSA en AP's
DC02	Domain Controller / Printserver / DNS / Radius server	2	8	320	Oude Printserver, Radius tbv SonicWalls, Citrix Gateway, Fileserver tbv Citrix Profielen
MON01	Ivensys / ArchestrA License Manager / SQL Server / Wonderware Historian	2	4	150	Data verzameling van Turbine PCs, drivemapping naar SFTP server
PRINT01	Printserver / Toshiba eFollow	2	4	60	Printserver

Tabel 12 – Verouderde servers

In het adviesrapport zal een advies gegeven worden welke servers vervangen dienen te worden en welke servers uitgefasseerd kunnen worden, indien deze niet meer benodigd zijn.

7.3.2 Huidige manier van werken

In de huidige omgeving wordt gewerkt vanuit twee verschillende omgevingen. Een klein aantal gebruikers maakt gebruik van Citrix voor het raadplegen van archiefdata (SAP) en het gebruik van generieke applicaties, zoals Microsoft Edge en Office. De overige gebruikers maken gebruik van laptops en desktops met daarop geïnstalleerde applicaties. Er wordt dus zowel lokaal gewerkt als in een Citrix omgeving.

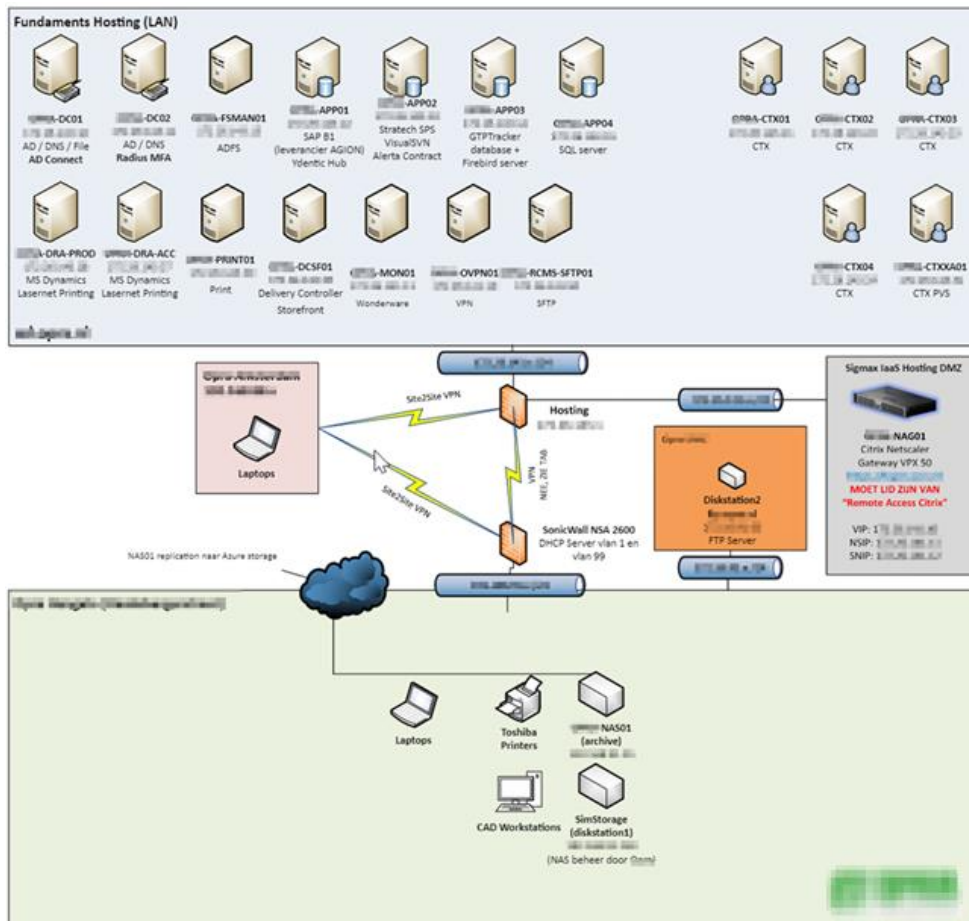
In onderstaande tabel is het huidige serverlandschap in kaart gebracht.

Servernaam	Rol/Functie
APP01	SAP Business One, Variatec Project Plus, FileZilla FTP server, Trimergo

APP02	VisualSVN Server, SQL Express, OfficeScan XG
APP03	Firebird SQL server, Tcserver, GPT Tracker import service
APP04	SQL Server
CTX01	Citrix Session Host
CTX02	Citrix Session Host
CTX03	Citrix Session Host
CTX04	Citrix Session Host
CTXXA01	Citrix Session Host
DC01	Domain Controller, Fileserver, PDM Vault
DC02	Domain Controller, Printserver, e-Follow print solution
DCSF01	Citrix Delivery Controller, Citrix Storefront
FSMAN01	ADFS
DRA-ACC	Microsoft Dynamics365 - Lasernet printing oplossing
DRA-PROD	Microsoft Dynamics365 - Lansenet printing oplossing
PRINT01	Printserver
MON01	SQL Server, Orchestra (Historian) license server, Invensys License Manager, WonderWare
NAG01	Citrix Netscaler
OVPN01	OpenVPN server t.b.v. turbines
RCMS-SFTP01	SFTP

Tabel 13 - Huidige serverlandschap

Om de huidige situatie goed te visualiseren is in figuur 11 de huidige omgeving in kaart gebracht. Vanwege privacy zijn alle IP-adressen gemaskeerd. In de tekening is de Fundaments Hosting (LAN) de private cloud omgeving.



Figuur 11 – Huidige situatie

7.4 Nieuwe situatie

Het uitgangspunt in de nieuwe situatie is om de requirements te verwerken in het ontwerp en de nieuwe situatie zo eenvoudig mogelijk op te zetten om onnodige resources te voorkomen. Ook is het van belang om de beveiliging van de apparaten van de eindgebruikers te verbeteren.

7.4.1 Inrichting Intune

De huidige werkplekken, bestaande uit laptops en desktops, zijn niet voldoende voorzien van beheer oplossingen om bijvoorbeeld beveiligingsmaatregelen door te voeren of de eindgebruiker te kunnen ondersteunen bij de uitgifte of herinstallatie van het apparaat. Dit is een risico, omdat op de laptops en desktops veel data opgeslagen staan en uit onderzoek is gebleken dat 85% van de datalekken veroorzaakt wordt door menselijke fouten zonder duidelijk beveiligingsbeleid.

Om de laptops en desktops naar het minimale niveau van beveiliging te brengen dienen er een aantal configuraties ingericht te worden in Intune. Exite maakt gebruik van een baseline Device Security, welke is opgedeeld in twee levels. Level 1 is een baseline met de minimale en vereiste inrichting van Intune en level 2 is een optionele inrichting als aanvulling op de level 1 baseline. De huidige inrichting voldoet daar momenteel niet aan.

De configuraties die ingericht moeten worden zijn conform de baseline Device Security van Exite en is te zien in onderstaande tabellen.

Vereiste configuraties

Maatregel	Omschrijving	Voorwaarden
Self-Service password reset & protection + User lock-out policy		
Microsoft Endpoint Manager (Intune)		Microsoft 365 Business Premium / Microsoft Enterprise Mobility + Security E3
Alle organisatie apparatuur is managed en voldoet aan compliance policy	Indien een apparaat niet voldoet, wordt toegang geblokkeerd tot resources.	
Bitlocker is ingeschakeld	Encryptie dataschijven	TPM 2.0 module (hardware)
Screenlock na x periode	Standaard: 5 minuten	
Password policy enabled	Minimaal 8 karakters, bij voorkeur 10 of 12. Verloopt niet of jaarlijks.	
Conditional access stap 2	Standaard toegang met MFA.	Microsoft 365 Business Premium / Microsoft Enterprise Mobility + Security E3
Block access Teams/OneDrive/SharePoint unmanaged devices		Microsoft 365 Business Premium / Microsoft Enterprise Mobility + Security E3
Block access Exchange Online Active sync unmanaged devices		Microsoft 365 Business Premium / Microsoft Enterprise Mobility + Security E3
Defender for Endpoint (ATP) of andere AV	Anti-virus	Defender for Endpoint Plan 1 / Defender for Endpoint Plan 2 / N-able

Tabel 14 - Vereiste configuraties Intune

Optionele configuraties

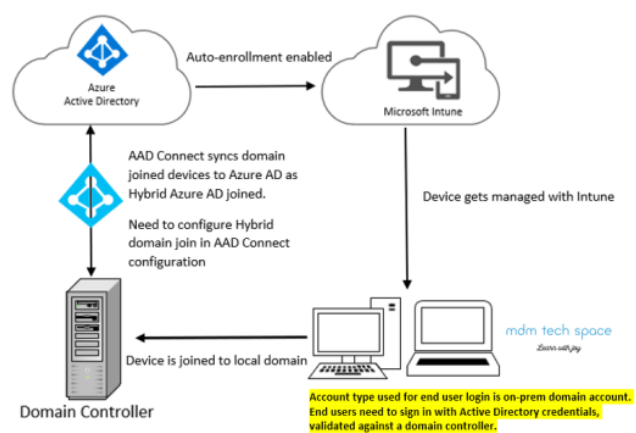
Maatregel	Omschrijving	Licentie voorwaarde
Mobile Application Management	Applicaties worden centraal uitgegeven. Installeren van applicaties door eindgebruikers wordt geblokkeerd.	Microsoft 365 Business Premium / Microsoft Enterprise Mobility + Security E3

Office 365 email encryption (AIP for Office)		Microsoft 365 Business Premium / Microsoft Enterprise Mobility + Security E3
Datalossprotection (DLP)	Opzetten van een DLP-beleid en toepassing in Sharepoint.	Microsoft 365 Business Premium / Microsoft Enterprise Mobility + Security E3
Windows Hello	Configureren Windows Hello voor authenticatie apparaat.	Microsoft 365 Business Premium / Microsoft Enterprise Mobility + Security E3

Tabel 15 – Optionele configuraties Intune

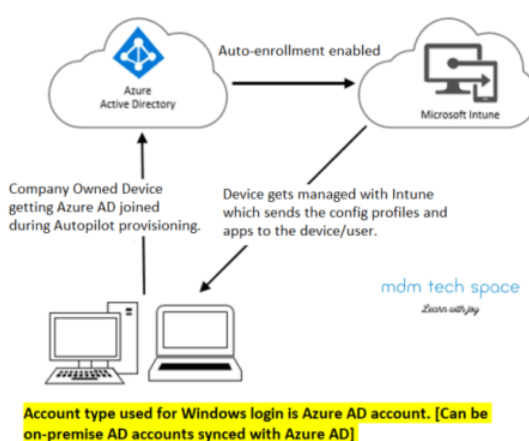
Hybride of Azure AD gekoppeld

Apparaten van eindgebruikers, de laptops en desktops, worden middels een hybride opstelling gekoppeld aan de Microsoft Cloud door middel van Intune. Dit heeft als voordeel dat huidige apparaten niet aangepast hoeven te worden door medewerkers van Exite om het device te laten werken met Intune. Al deze werkzaamheden gebeuren achter de schermen. Dit houdt in dat het device Hybride Joined gemaakt wordt met de Microsoft Cloud waarin Intune zich bevindt. Hierdoor heeft de eindgebruiker geen hinder in de werkzaamheden. In figuur 12 is te zien hoe deze opstelling eruit ziet.



Figuur 12 – Hybride Joined

De Intune omgeving wordt echter wel geschikt gemaakt om zonder hybride opstelling te kunnen werken voor toekomstig nieuw uit te leveren laptops en desktops. Dan wordt het device alleen nog Azure AD joined en heeft het geen directe afhankelijkheden meer met het lokale Windows netwerk. Dit heeft verder geen impact op de eindgebruikers, omdat dit alleen geldt voor nieuw uit te leveren apparaten. In figuur 13 is deze Intune omgeving te zien, zonder afhankelijkheden van het lokale Windows netwerk.



Figuur 13 – Azure AD Joined

7.4.2 Data migreren naar OneDrive en Teams/SharePoint

Uit de analyse is gebleken dat alle data momenteel op veel verschillende locaties wordt opgeslagen op verschillende fileshares. Om dit te optimaliseren zal alle data gemigreerd worden naar OneDrive en Teams/SharePoint. Dit heeft als voordeel dat de data, welke op de servers in de private cloud staat, ook te benaderen is zonder gebruikt te maken van Citrix of VPN. Wel is het noodzakelijk dat het apparaat van de eindgebruiker voldoet aan de compliance policy, anders wordt er geen toegang verkregen tot de data, zoals beschreven in de baseline Device Security. Er zal wel onderzocht moeten worden of alle data geschikt is voor OneDrive en Teams/SharePoint. Hiervoor zal aanvullend onderzoek benodigd zijn.

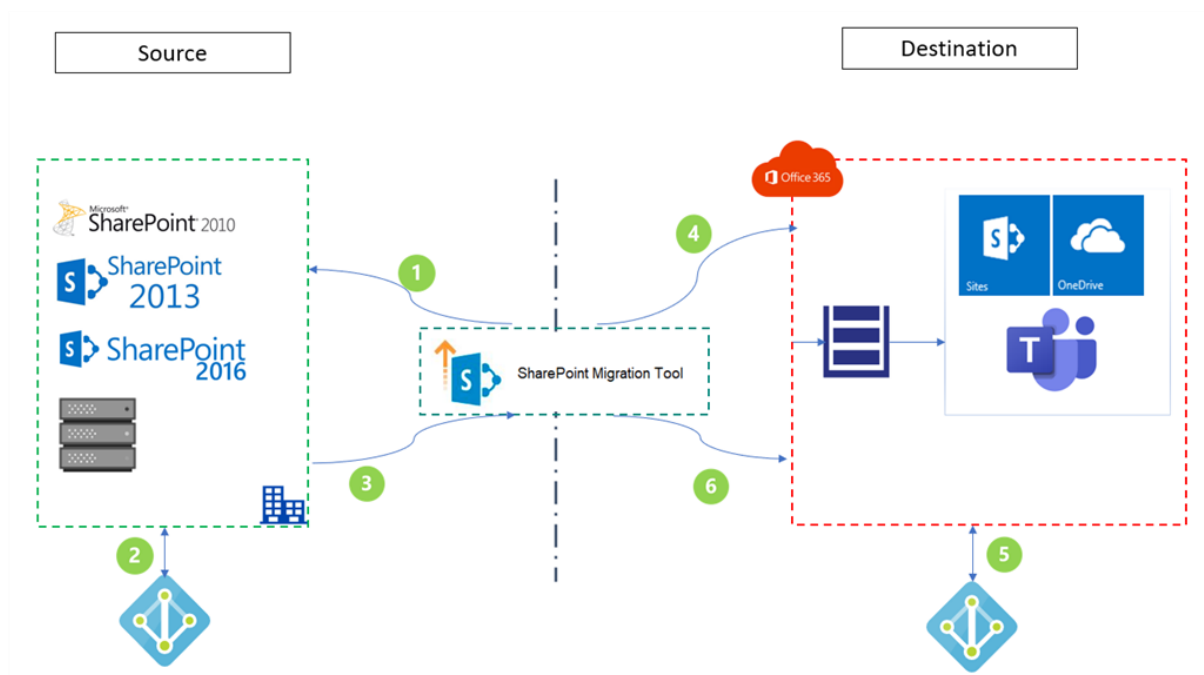
OneDrive

Alle persoonlijke data van de eindgebruikers zal worden gemigreerd naar OneDrive. Elke eindgebruiker heeft een persoonlijke OneDrive opslag welke gekoppeld is aan het Office365 account van de eindgebruiker. Op de apparaten zal een map in de verkenner komen, waardoor alle persoonlijke data direct te benaderen is.

Teams/SharePoint

Alle data welke door meerdere eindgebruikers inzichtelijk moet zijn of aangepast moet worden zal worden gemigreerd naar Teams/SharePoint. Hierin kunnen verschillende teams/sites aangemaakt worden per afdeling of functiegroep. Op deze wijze is er controle en grip over wie toegang heeft tot welke data. Door gebruik te maken van Teams/SharePoint is het mogelijk om tegelijk samen te werken in documenten. Hierdoor voorkom je verschil in versies van bestanden en data dat mogelijk niet actueel is.

Om al deze data goed en veilig te kunnen migreren naar de cloud wordt gebruik gemaakt van de Microsoft SharePoint Migration Tool (SPMT). Figuur 14 laat zien hoe deze tool ingezet dient te worden. Middels een CSV-bestand kunnen de huidige en nieuwe opslag locaties opgegeven worden en op deze wijze zorgt de SPMT ervoor dat op het gewenste tijdstip alle data stuk voor stuk gemigreerd wordt naar Teams/SharePoint. Hierdoor wordt de downtime geminimaliseerd.



Figuur 14 – Microsoft SharePoint Migration Tool

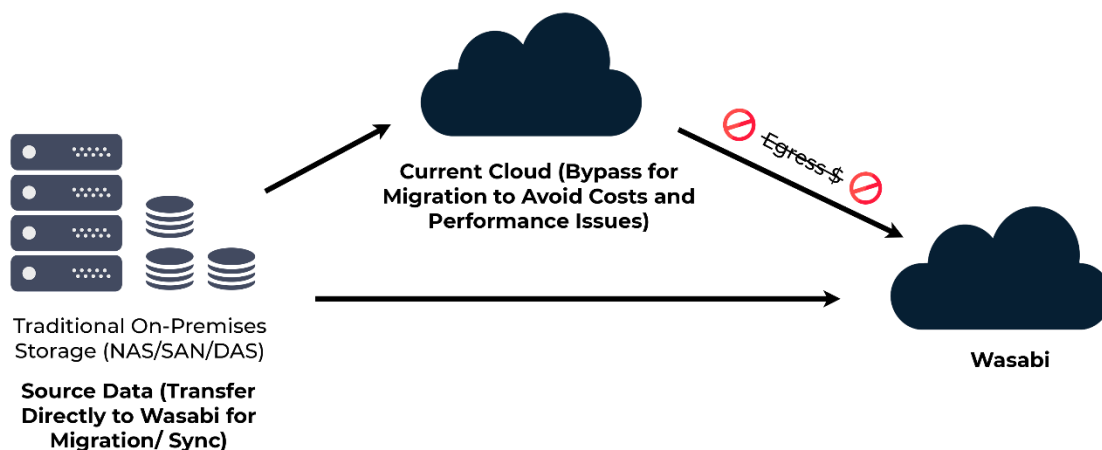
7.4.3 NAS uitfaseren en migreren naar Wasabi

Er wordt momenteel nog gebruik gemaakt van een NAS op locatie, hierop is een grote hoeveelheid archief data opgeslagen. Deze NAS wordt momenteel beheerd door de klant zelf. Deze apparaten hebben geen eindeloos leven en zal op termijn vervangen moeten worden.

Uit onderzoek is gebleken dat Wasabi Cloud NAS veel voordelen biedt ten opzichte van een on-premise NAS. Het nadeel is dat de data in de public cloud staat, maar weegt niet op tegen de voordelen die deze dienst te bieden heeft. De archiefdata zal gemigreerd worden naar een Wasabi Cloud NAS oplossing, waarbij deze data eenvoudig en vanaf elke apparaat toegankelijk gemaakt kan worden. Tevens krijgt de klant daarbij de mogelijkheid om de huidige data eenvoudig en geautomatiseerd te archiveren naar Wasabi Cloud storage. Ook zal de migratie naar de Wasabi Cloud NAS ervoor zorgen dat alle archiefdata beschermd is tegen ransomware aanvallen, wat de beveiliging ten goede doet.

Door de implementatie van Wasabi Cloud NAS en migratie naar OneDrive/Teams/SharePoint is er ook geen fileserver meer benodigd, waardoor deze inrichting ook kostenbesparend is.

Om alle data van de on-premise NAS te migreren naar de Wasabi Cloud NAS kan de migratie tool van Wasabi gebruikt worden. In figuur 15 is te zien hoe deze migratie er uit zal zien. De on-premise NAS kan direct verbonden worden met de Wasabi Cloud NAS, waardoor de data migratie snel en eenvoudig plaatsvindt op het gewenste tijdstip, waardoor de downtime minimaal is.



Figuur 15 – Migratie Wasabi Cloud NAS

7.4.4 Uutfaseren Citrix omgeving

Om de Citrix omgeving in de private cloud uit te faseren, zullen er aan aantal servers uitgefaseerd worden. Uit het onderzoek in bijlage E – Onderzoek huidige omgeving, is gebleken dat de huidige Citrix omgeving is verouderd en end-of-life is. In de nieuwe situatie zal Citrix volledig uitgefaseerd worden en vervangen worden door een RDS oplossing. Deze omgeving wordt door een klein aantal gebruikers gebruikt en is vergelijkbaar met Citrix, waardoor een RDS oplossing beter past dan Citrix. Door gebruik te maken van een nieuwe RDS oplossing zijn er op termijn 6 servers minder benodigd dan in de huidige situatie. Op deze nieuwe RDS server zal de SAP client geïnstalleerd worden en een aantal generieke applicaties. Alle overige applicaties kunnen op de laptops en desktops geïnstalleerd worden indien deze nodig zijn. Onderstaande Citrix servers zullen worden uitgefaseerd:

Servernaam	Rol	CPU	RAM	HDD	Opmerking
DCSF01	Delivery Controller / Storefront / License Server	2	8	100	Server 2012 R2
CTX01	Session Host	6	32	100	Server 2012 R2
CTX02	Session Host	6	32	100	Server 2012 R2
CTX03	Session Host	6	32	100	Server 2012 R2
CTX04	Session Host	6	32	100	Server 2012 R2
CTXXA01	Session Host	2	4	60	Server 2012 R2, Test server
NAG01	Citrix Gateway / Netscaler	2	8	20	T.b.v. externe toegang

Tabel 16 – Citrix servers

Onderstaande nieuwe RDS server zal worden geïnstalleerd met Windows Server 2022:

Servernaam	Rol/Functie	CPU	RAM	HDD	Opmerking
RDS01	RDS	4	24	100	t.b.v. SAP en overige generieke applicaties

Tabel 17 – RDS server

Mocht op den duur één RDS server niet voldoende zijn om de eindgebruikers voldoende te faciliteren, kan er gemakkelijk een RDS servers toegevoegd worden. Op deze manier is de omgeving ook schaalbaar.

7.4.5 Nieuwe situatie

In dit kopje wordt de nieuwe situatie in kaart gebracht. Om de nieuwe omgeving van de klant zo eenvoudig mogelijk op te zetten worden een aantal servers uitgefaseerd en vervangen. In het adviesrapport wordt een toelichting gegeven op welke servers vervangen worden en welke servers uitgefaseerd worden. In onderstaande tabel is de nieuwe serveromgeving te zien. Hierin is de Citrix omgeving uitgefaseerd en vervangen door een nieuwe RDS omgeving en zijn verschillende servers uitgefaseerd. Door deze uitfasering heeft de klant minder kosten op het gebied van resources.

Servernaam	Rol/Functie	CPU	RAM	HDD	Opmerking
APP01	SQL Server (SAP)	2	16	150	SAP databases / Radius server
APP02	MySQL / OpenVPN / TCserver / GTP Tracker	4	4	40	
DC01	Domain Controller / DNS	2	8	80	
DRA-ACC	Dynamics Acceptatie	2	16	80	
DRA-PROD	Dynamics Productie	2	16	80	
MON01	Ivensys / Archestra License Manager / SQL Server / Wonderware Historian	2	4	150	Data verzameling van Turbine PCs, drivemapping naar SFTP server
FS01	File- / printserver	2	8	3600	
RDS01	RDS	4	24	100	t.b.v. SAP en overige generieke applicaties
OVPN01	VPN Server turbines	2	8	60	
RCMS-SFTP01	Secure FTP Server	2	8	60	

Tabel 18 - Nieuw serverlandschap

Om de nieuwe situatie goed te visualiseren is in bijlage F – Nieuwe situatie de nieuwe omgeving in kaart gebracht.

7.5 Conclusie

Uit het ontwerp kan geconcludeerd worden dat de huidige omgeving erg complex is opgezet en dat de inrichting van de werkplekken niet voldoende beveiligd is. Ook zijn er meerdere servers welke niet meer in gebruik zijn en is de bestaande Citrix omgeving verouderd en te ruim opgezet ten opzichte van het gebruik. Uit het ontwerp blijkt dat er veel optimalisaties mogelijk zijn en deze resultaten van het ontwerp zullen de input vormen van het advies wat gegeven wordt aan Exite.

8 Advies

Het adviesrapport geeft antwoord op de deelvraag “Hoe kan Exite de mogelijke cloudoplossing implementeren?”

8.1 Methodiek

Op basis van de resultaten van het ontwerp wordt er in dit hoofdstuk een advies gegeven hoe de gewenste oplossing ingericht kan worden.

8.2 Resultaten

Om klanten naar de cloud te migreren is het advies aan Exite om daar een generieke methodiek voor te hanteren. Uit onderzoek is gebleken dat de 6R-methode veel voordelen biedt om een cloudmigratie tot een succes te brengen. Een kritische succesfactor en tevens het advies aan Exite is om een cloudmigratie uit te voeren in verschillende fases.

Om de huidige omgeving van de specifieke klant te optimaliseren en concrete vervolg acties te verbinden aan de conclusies is het advies aan Exite om de optimalisatie en migratie uit te voeren in onderstaande fases. Op deze wijze zal de migratie stapsgewijs verlopen en de minste impact veroorzaken.

- ✕ Fase 1: Afschalen Citrix en server omgeving
- ✕ Fase 2: Implementatie van Intune en migratie NAS naar Wasabi Cloud NAS
- ✕ Fase 3: Migratie data op fileshares naar OneDrive, Teams en SharePoint
- ✕ Fase 4: Vervanging verouderde Windows servers en implementatie RDS

8.2.1 Fase 1 – Afschalen Citrix en server omgeving

De huidige Citrix omgeving is in de periode maart 2023 tot en met april 2023 gebruikt door 26 gebruikers. Dagelijks zijn er niet meer dan 5 gebruikers tegelijk ingelogd op de Citrix servers. Tevens zijn er een aantal servers welke minder resources nodig hebben, omdat van deze systemen ook minder gebruik wordt gemaakt zoals de SQL server voor SAP (APP01), of lijken helemaal niet meer actief worden gebruikt omdat er andere software oplossingen zijn ingezet.

Afschalen resources private cloud

Om bovenstaande redenen is het advies om onderstaande servers af te schalen en te voorzien van minder resources, deze servers worden niet uitgeschakeld of uitgefaseerd, omdat deze nog een rol van betekenis hebben. Door deze resources af te schalen kunnen kosten bespaard worden. Mocht het blijken dat er teveel is afgeschaald, waardoor applicaties traagheid ondervinden, zijn deze resources gemakkelijk op te schalen, wat de omgeving schaalbaar maakt.

Servernaam	Rol/Functie	CPU	RAM	HDD	Opmerking
APP01	SAP SQL Server, Exchange Management	2	16	350	Was voorzien van 4 CPU en 32 GB RAM.
APP03	MySQL, OpenVPN, TCserver, GTP Tracker	4	4	40	D: schijf van 100 GB verwijderen (niet in gebruik)

Tabel 19 – Af te schalen resources

Afschalen server omgeving

Het advies aan Exite is om de volgende servers eerst uit te schakelen en na een maand te verwijderen. Indien nodig kunnen deze nog hersteld worden uit de back-up. Op deze manier voorkom je dat er mogelijk teveel wordt uitgefasseerd.

Servernaam	Rol/Functie	CPU	RAM	HDD	Opmerking
APP02	Stratech SPS SQL Server, SVN Server (Tortoise)	2	8	100	Niet meer benodigd
APP04	SQL Server	2	8	100	Niet meer benodigd
CTX02	Citrix Desktop	6	32	100	Niet meer benodigd
CTX03	Citrix Desktop	6	32	100	Niet meer benodigd
CTX04	Citrix Desktop	6	32	100	Niet meer benodigd
CTXXA01	Citrix Desktop	2	4	60	Niet meer benodigd

Tabel 20 – Af te schalen servers

Voor de Citrix omgeving blijft er na deze fase en aanpassing nog één Citrix server over om een virtuele desktop met onder andere de SAP client en overige software aan te kunnen bieden voor gebruikers welke dit nog nodig hebben. De overige Citrix servers worden uitgeschakeld, omdat deze niet benodigd zijn voor de hoeveelheid gebruikers die tegelijk verbinding maken met de virtuele desktop. Het volledig vervangen van de Citrix omgeving voor een RDS omgeving zal in een latere fase aan bod komen.

8.2.2 Fase 2 – Implementatie van Intune en migratie NAS naar Wasabi Cloud NAS

De huidige werkplekken, bestaande uit laptops en desktops, zijn niet voldoende voorzien van management oplossingen om bijvoorbeeld beveiligingsmaatregelen door te voeren of de gebruiker te ondersteunen bij de uitgifte of herinstallatie van het apparaat. Dit vormt een risico, omdat op de laptops en desktops veel data staat opgeslagen. Ook in het geval van diefstal van laptops vormt dit een risico, laptops kunnen op afstand niet worden gewist.

Uit het onderzoek in bijlage E – Onderzoek huidige omgeving is gebleken dat de klant gebruik maakt van Office 365 E3 en Azure AD Premium P1 licenties. Het advies is om deze twee licenties om te zetten naar één Microsoft Business Premium licentie. Op korte termijn kunnen hierdoor de Office 365 E3 licenties afgeschaald worden. Deze licentie is specifiek bedoelt voor organisaties tot 300 gebruikers en biedt naast de functies uit licenties zoals Office 365 E3 en Azure AD Premium nog extra

mogelijkheden voor een sterk gereduceerd maandelijks bedrag. De extra mogelijkheden uit Microsoft Business Premium zijn:

- ✗ Intune, t.b.v. apparaat management voor o.a. het op afstand beheren van laptops en desktops, installatie van applicaties, uitrol van beveiligingsbeleid op apparaat niveau, diverse configuratie instellingen
- ✗ AutoPilot t.b.v. self-service uitrol van apparaten door eindgebruikers, geen technisch support meer nodig
- ✗ Defender for Office t.b.v. anti-virus, anti-spam, anti-phishing voor e-mail, OneDrive, Teams/Sharepoint data
- ✗ Defender for Business t.b.v. anti-virus op Windows apparaten

Door gebruik te maken van deze nieuwe mogelijkheden, waarbij het beveiligingsniveau voor mail, data in Microsoft cloud (OneDrive, Teams en SharePoint) en de laptops en desktops waarmee gebruikers werken naar een hoger niveau getild wordt tijdens deze fase de basis inrichtingen van Exite geïmplementeerd.

Hybride of Azure AD gekoppeld

Het advies aan Exite is om alle apparaten te koppelen aan Intune, middels een Hybride Joined opstelling. Op deze manier kunnen apparaten verbinding maken met Intune en zal dit volledig achter de schermen gebeuren. Eindgebruikers ervaren hier geen hinder van en de vereiste configuraties, zoals beschreven in de baseline Device security, kunnen door de engineers van Exite in Intune geïmplementeerd worden. Deze configuraties zullen op de achtergrond gepusht worden naar de apparaten.

Het advies is wel om de Intune omgeving zodanig in te richten dat nieuwe apparaten middels een Azure AD koppeling verbinding kunnen maken met Intune. Op deze manier benutten de nieuwe apparaten alle voordelen van de Azure AD koppeling, zoals beschreven in de afweging. Hierdoor worden op de lange termijn alle apparaten Azure AD gekoppeld met de Intune omgeving.

Afweging

Om alle apparaten (laptops en desktops) niet langer afhankelijk te maken van Domain Controllers in het netwerk van de klant, wordt bij het maken van deze optionele keuze, alle Windows apparaten Azure AD Joined uitgevoerd. Dit betekent dat het apparaat opnieuw wordt geïnstalleerd en voorzien van Windows 11 Business op apparaten waar nu minimaal Windows 10 is geïnstalleerd.

Door apparaten Azure AD Joined uit te voeren vindt de authenticatie plaats naar de Microsoft Cloud in plaats van naar een Windows server. Dit heeft de volgende voordelen:

- ✗ Cloud native, geen afhankelijkheden met on-premises of private cloud omgeving
- ✗ Authenticatie vindt plaats naar de Microsoft Cloud in plaats van naar Windows servers
- ✗ Uitgeschakelde gebruikersaccounts of apparaten zijn direct van kracht en overal ter wereld direct doorgevoerd

- ✗ Wachtwoord wijzigingen zijn direct van kracht en overal ter wereld direct doorgevoerd
- ✗ Toekomst bestendig
- ✗ Apparaat hoeft zich niet langer te bevinden in het netwerk van de klant bij herinstallatie
- ✗ Biedt mogelijkheden voor Windows Hello for Business t.b.v. biometrische authenticatie
- ✗ Self-service herinstallatie

Het nadeel is dat de klant specifieke applicaties opnieuw geïnstalleerd moeten worden aangezien er een breed scala aan gebruiker specifieke applicaties en applicatieversies worden gebruikt.

Microsoft 365 back-up

Mailboxen, OneDrive en Teams/SharePoint data worden op dit moment niet in een back-up meegenomen. Het advies is om de data binnen Microsoft 365 wel te back-uppen. Door gebruik te maken van back-ups is het mogelijk om bijvoorbeeld data en/of e-mails die ten onrechte verwijderd zijn terug te halen. Ook in het geval van een phishing aanval middels de e-mail en de data en e-mail niet meer beschikbaar zijn is het mogelijk om deze vanuit de back-up terug te kunnen halen.

Migratie NAS naar Wasabi Cloud NAS

Het advies aan Exite is om de huidige on-premise NAS te migreren naar de Wasabi Cloud NAS oplossing. Hiermee is alle archiefdata welke daarop staat opgeslagen beveiligd tegen onder andere ransomware door de data immutable te maken. De archiefdata staat op deze manier extra veilig opgeslagen en de eindgebruikers kunnen de archiefdata gemakkelijk benaderen middels een fileshare op de laptops en desktops. Op deze manier is de archiefdata niet alleen te benaderen vanaf kantoorlocatie, zoals in de huidige situatie, maar ook vanuit externe locaties.

De Wasabi Cloud NAS kan eenvoudig opgezet worden door de on-premise NAS direct te verbinden met Wasabi. Alle data wordt dan automatisch gemigreerd. Voor de eindgebruikers zal er weinig veranderen, ze kunnen de nieuwe NAS benaderen middels een fileshare op de laptops en desktops.

8.2.3 Fase 3 – Migratie data op fileshares naar OneDrive, Teams en SharePoint

Uit de analyse is gebleken dat er veel data op veel verschillende plekken staat opgeslagen op verschillende fileshares. Het advies aan Exite is om deze data in samenwerking met de klant inzichtelijk te maken. Zodra deze data inzichtelijk is en het duidelijk is welke data waar bij hoort, kan de Teams/SharePoint omgeving worden ingericht door Exite. Vervolgens kan de data gemigreerd worden op het gewenste moment. Op deze manier kan iedereen met de juiste toegang bij de juiste bestanden komen. Hierdoor is op den duur ook minder opslag benodigd op de fileservers.

Om dit te kunnen realiseren zal aanvullend onderzoek moeten plaatsvinden in samenwerking met de klant.

8.2.4 Fase 4 – Vervanging verouderde Windows servers en implementatie RDS

Gedurende het onderzoek in bijlage E – Onderzoek huidige omgeving is gebleken dat er nog een aantal servers in de private cloud gebruik maken van Windows Server 2012 R2. Dit besturingssysteem

wordt vanaf oktober 2023 niet langer ondersteund door Microsoft en ontvangt dan geen ondersteuning en beveiligingsupdates meer. Om deze reden is het advies om het besturingssysteem te vervangen voor een recente versie, Windows Server 2022.

Overzicht servers om te vervangen

Het advies is om onderstaande servers te vervangen voor Windows Server 2022, waarbij deze servers opnieuw geïnstalleerd moeten worden., hierbij is mogelijk ondersteuning van leveranciers van de applicaties benodigd.

Servernaam	Rol/Functie	CPU	RAM	HDD	Opmerking
APP01	SQL Server (SAP) / Exchange Management	2	16	150	SAP databases / Radius server
APP03	MySQL / OpenVPN / TCserver / GTP Tracker	4	4	40	Wordt na herinstallatie APP02
DC01	Domain Controller / Fileserver / DNS / DHCP / Radius server	2	8	3600	
MON01	Ivensys / Archestra License Manager / SQL Server / Wonderware Historian	2	4	150	Data verzameling van Turbine PCs, drivemapping naar sftp server
PRINT01	Printserver / Toshiba e-Follow	2	8	3600	File-/ Printserver Wordt na herinstallatie FS01

Tabel 21 - Te vervangen servers

Uitfasering Citrix en implementatie RDS

Deze fase wordt ook direct gebruikt om de overgebleven Citrix omgeving te vervangen voor een Remote Desktop (RDS) oplossing, omdat deze op dit moment beter aansluit en Citrix geen meerwaarde meer biedt. Door de implementatie van RDS zijn er vervolgens minder servers benodigd in de private cloud. Het advies is om onderstaande servers uit te faseren, omdat ze niet langer nodig zijn door de implementatie van de RDS server.

Servernaam	Rol/Functie	CPU	RAM	HDD	Opmerking
DCSF01	Delivery Controller / Storefront / License Server	2	8	100	Server 2012 R2
CTX01	Session Host (desktop)	6	32	100	Server 2012 R2
NAG01	Citrix Gateway / Netscaler	2	8	20	t.b.v. externe toegang
DC02	Domain Controller / Printserver / DNS / Radius server	2	8	320	Oude Printserver, Citrix Gateway, Fileserver t.b.v. Citrix Profielen

Tabel 22 - Uitfasering Citrix

Ook zal in deze fase de nieuwe RDS server, benoemd in het ontwerp, worden geïmplementeerd, ter vervanging van de huidige Citrix omgeving, op basis van Windows Server 2022. Door de implementatie van RDS is de Citrix omgeving niet meer benodigd en vergt dit minder servers.

8.2.5 Afweging

De afweging die gemaakt kan worden is om de volledige nieuwe omgeving in de private cloud te migreren naar de public cloud in Azure. Om dat te realiseren is aanvullend onderzoek benodigd. Er zal een aanvullend onderzoek uitgevoerd moeten worden naar de kosten van de nieuwe private cloud omgeving en een kostenindicatie van de mogelijke Azure omgeving.

Ook zal er in het aanvullende onderzoek gekeken moeten worden of er van bestaande applicaties eventueel SaaS-diensten beschikbaar zijn, wat ervoor kan zorgen dat er minder servers benodigd zijn en deze applicaties direct vanuit de public cloud aangeboden kunnen worden.

8.3 Advies en conclusie

In de laatste fase van dit onderzoek is een advies gegeven aan Exite over hoe het opgestelde ontwerp gerealiseerd kan worden. Dit advies geeft antwoord op de laatste deelvraag “Hoe kan Exite de mogelijke cloudoplossing implementeren?”.

Uit het advies kan geconcludeerd worden dat het volledig migreren van de omgeving naar een public cloud oplossing geen mogelijkheid of toegevoegde waarde is. De huidige omgeving kan wel op veel vlakken geoptimaliseerd worden om het werken efficiënter, flexibeler en veiliger te maken. Gedurende het onderzoek is gekeken naar de mogelijkheden om de huidige omgeving te optimaliseren en de conclusie is dat Exite het huidige serverlandschap kan reduceren en vernieuwen. De Citrix omgeving kan uitgefasseerd worden en vervangen worden door een vernieuwende RDS oplossing en verouderde servers kunnen vervangen worden. Dit zal beter aansluiten bij de huidige manier van werken, zoals beschreven in hoofdstuk 7.3.2.

Voor het succes van een optimalisatie en/of cloudmigratie is het essentieel dat de eindgebruikers vanaf het begin betrokken zijn bij de oplossing. Tot slot is het van belang om eindgebruikers te helpen wennen aan en te leren werken via de cloud en is het belangrijk om de optimalisatie en/of migratie in behapbare stappen/fases te implementeren.

Om echt volledig naar een public cloud oplossing te migreren zal aanvullend onderzoek benodigd zijn. Per applicatie moet onderzocht worden, middels het generieke 6R-model, of de applicatie geschikt is voor de public cloud en mogelijk als SaaS-oplossing aangeboden kan worden. Hiervoor zal ook met leveranciers gesproken moeten worden. Indien er applicaties als SaaS-oplossing beschikbaar zijn is dat een mogelijkheid om een migratie uit te voeren naar Azure. Dit aanvullende onderzoek is in dit project niet aan bod gekomen, omdat de omgeving veel verschillende applicaties betreft en het niet duidelijk is welke applicaties daadwerkelijk nog gebruikt worden of niet.

Verder kan Exite door gebruik te maken van de Wasabi Cloud NAS oplossing werken naar een hybride cloud omgeving. Hierdoor behoud je het vernieuwde serverlandschap en wordt de on-

premise NAS gemigreerd naar een public cloud oplossing. Dit biedt veel voordelen voor de klanten van Exite.

9 Ontwerpevaluatie

Op basis van de opgestelde requirements wordt er per requirement aangegeven of deze is behaald in dit onderzoek. In onderstaande tabel worden de user requirements weergegeven met het behaalde resultaat van het onderzoek.

Nr.	Beschrijving	F/NF	Prioriteit	Resultaat
U01	De solution architecten zullen het ontwerp bij verschillende klanten met complexe on-premise omgevingen, welke in een private cloud staan, kunnen implementeren.	F	Should	Geslaagd, het ontwerp is bij verschillende klanten met soortgelijke omgevingen te implementeren.
U02	De beheerders moeten de oplossing kunnen beheren, door wijzigingen uit te kunnen voeren.	F	Must	Geslaagd, Exite kan de nieuwe situatie zelf inrichten en zelf beheren.
U03	De solution architecten moeten een advies krijgen hoe de on-premise omgeving, welke in een private cloud staat, gemigreerd kan worden naar de public en/of hybride cloud.	NF	Must	Geslaagd, in het advies wordt aangegeven hoe de huidige omgeving te migreren is naar een hybride cloud oplossing.
U04	De solution architecten moeten een advies krijgen of de huidige omgeving van de klant te migreren is naar een public en/of hybride cloudomgeving.	NF	Must	Geslaagd, in het advies wordt aangegeven of de huidige omgeving te migreren is naar een public en/of hybride cloud.
U05	De solution architecten moeten een ontwerp krijgen, waarin de huidige situatie en de nieuwe situatie wordt beschreven.	F	Must	Geslaagd, in het ontwerp is een huidige- en nieuwe situatie beschreven en gevisualiseerd.
U06	De solution architecten moeten een overzicht krijgen van de verbeteringen van de gewenste situatie ten opzichte van de huidige situatie.	NF	Must	Geslaagd, in het ontwerp en advies wordt beschreven welke optimalisaties doorgevoerd kunnen worden in de huidige omgeving.
U07	De solution architecten moeten een ontwerp krijgen, waarin het huidige applicatielandschap in kaart gebracht wordt.	F	Should	Geslaagd, in het ontwerp is een overzicht te zien op welke server welke applicaties staan.
U08	Voor het succes van een cloudmigratie is het essentieel dat de eindgebruikers vanaf het begin betrokken zijn bij de oplossing.	NF	Must	Geslaagd, in het advies wordt het advies gegeven eindgebruikers direct te betrekken.

Tabel 23 - Ontwerpevaluatie

10 Eindconclusie

Op basis van de opgestelde probleemstelling is een hoofdvraag geformuleerd. Om deze hoofdvraag te beantwoorden zijn onderstaande deelvragen geformuleerd.

10.1 Beantwoording deelvragen

In dit hoofdstuk worden de deelvragen beantwoord.

10.1.1 Deelvraag 1: Wat is de definitie van cloudcomputing?

Cloudcomputing is het leveren van computingservices, inclusief servers, opslag, databases, netwerkfuncties, software, analysefuncties en intelligentie, via internet waarmee snellere innovatie, flexibele resources en schaalvoordelen beschikbaar is. Cloudcomputing biedt voordelen op het gebied van kosten, wereldwijde schaalbaarheid, prestaties, beveiliging, snelheid, productiviteit, en betrouwbaarheid.

10.1.2 Deelvraag 2: Wat zijn de mogelijkheden met betrekking tot een migratie naar de cloud?

Allereerst moet het type cloudimplementatie of cloudcomputingarchitectuur bepaald worden waarop de cloudservices worden geïmplementeerd. Er zijn drie verschillende manieren om cloudservices te implementeren: in een public cloud, private cloud of hybride cloud. Een mix van deze drie mogelijkheden behoort ook tot de opties.

10.1.3 Deelvraag 3: Wat moet er gedaan worden om ervoor te zorgen dat de beveiliging in de cloud voldoende is?

Om de cloud omgeving goed te kunnen beveiligen en veilig te houden zijn er een aantal best practices waar rekening mee gehouden moet worden.

- ✕ Ken en visualiseer de gegevens
- ✕ Kies de juiste cloudprovider
- ✕ Houd rekening met wettelijke eisen
- ✕ Versleuteling op bestandsniveau
- ✕ Beveilig apparaten van eindgebruikers
- ✕ Gebruik best practices voor wachtwoorden
- ✕ Gebruik twee-factorverificatie
- ✕ Veilige gegevens overdracht
- ✕ Maak back-ups van gegevens

10.1.4 Deelvraag 4: Hoe kan een cloudoplossing schaalbaar worden gemaakt?

Schaalbaarheid is een systeem dat snelle veranderingen in werklast en vraag kan verwerken. De schaalbaarheid geeft aan hoe goed dat systeem reageert op veranderingen door resources toe te

voegen of te verwijderen om aan de vraag te voldoen. Een cloudoplossing kan schaalbaar gemaakt worden door middel van horizontaal schalen en verticaal schalen. Horizontaal schalen houdt in dat er simpelweg VM's worden toegevoegd en verticaal schalen houdt in dat de bestaande VM omhoog geschaald wordt met extra resources.

Ook is het mogelijk om resources automatisch te schalen. Automatisch schalen voegt resources toe of schaaft deze juist af om piekbelastingen, zoals seizoensgebonden workloads, effectief aan te kunnen.

10.1.5 Deelvraag 5: Welke gevolgen zou een migratie naar de cloud met zich mee brengen voor de klant?

Cloudmigraties hebben altijd gevolgen op voornamelijk de eindgebruikers, omdat zij er immers mee moeten kunnen werken. Het gebrek aan grondige overweging leidt tot onvoorspelbare kosten en een aanzienlijk risico op een teleurstellende cloudimplementatie die niet aan de verwachtingen voldoet. Bovendien is het tijdstip waarop je overstapt naar de cloud ook van invloed. Een verstandig moment hiervoor is bijvoorbeeld wanneer je bedrijf aanzienlijke groei doormaakt en behoefte heeft aan schaalbare diensten. Een kritische evaluatie van welke systemen geschikt zijn voor de cloud en welke eerst aangepast moeten worden, evenals het identificeren van toepassingen die offline moeten blijven werken, draagt bij aan een succesvolle migratie naar de cloud. Zonder deze kritische benadering kunnen de gevolgen groot zijn, zoals een grotere kans op datalekken en cyberaanvallen, onnodig hoge kosten en een niet stabiele cloudomgeving als gevolg van instabiele applicaties.

10.1.6 Deelvraag 6: Wat is de huidige IT-infrastructuur van de klant?

De huidige omgeving is complex ingericht. Er wordt gebruik gemaakt van een verouderde Citrix omgeving. Verder wordt er gebruik gemaakt van laptops, welke middels Microsoft Endpoint Manager zijn uitgerold. Momenteel is dit erg matig en minimaal ingericht en voldoet de inrichting niet aan de beveiligingseisen van Exite. Het volledige serverlandschap staat momenteel opgenomen in de private cloud. Verder staat op locatie een NAS, waarop veel archiefdata is opgeslagen.

10.1.7 Deelvraag 7: Wat zijn de knelpunten op het gebied van beveiliging?

Uit het literatuuronderzoek is gebleken dat de klant momenteel twee grote knelpunten heeft. De klant heeft een legacy omgeving waar ze moeilijk van af kunnen en ze hebben een Citrix omgeving, waar ze weinig van de Microsoft 365 facetten kunnen benutten. Dit houdt in dat de omgeving erg statisch is. Ook wordt er nog deels lokaal gewerkt. Dit houdt in dat er vanuit twee omgevingen gewerkt wordt. Veel data staat momenteel opgeslagen op verschillende locaties en er staat veel archiefdata opgeslagen op een lokale NAS. De beveiliging kan hierdoor niet 100% worden afgedicht en vormt een risico voor de klant.

10.1.8 Deelvraag 8: Wat zijn kritische succesfactoren om het project te doen slagen voor een klant?

Het belang van migratie naar een digitale werkomgeving moet duidelijk zijn voor de gehele organisatie. Een andere kritische succesfactor is het begrijpen waar je vandaan komt en waar je

naartoe wilt. Uit onderzoek is gebleken dat er is een duidelijk verschil is tussen hoe vroeger werd gewerkt en hoe het nu gaat. Verder blijkt het in de praktijk dat het beter is om specialistische taken toe te vertrouwen aan partijen die de kennis, vaardigheden en tools hebben en dit als dagelijkse activiteit uitvoeren. Voor het succes van een cloudmigratie is het essentieel dat de eindgebruikers vanaf het begin betrokken zijn bij de oplossing. Tot slot is het van belang om eindgebruikers te helpen wennen aan en te leren werken via de cloud, is het belangrijk om de migratie in behapbare stappen/fases te implementeren.

10.1.9 Deelvraag 9: Hoe kan Exite de mogelijk cloudoplossing implementeren?

Uit het advies is gebleken dat de implementatie van de cloudoplossing uitgevoerd dient te worden in vier fases. Op deze wijze zal de migratie stapsgewijs verlopen en de minste impact veroorzaken.

- ✕ Fase 1: Afschalen Citrix en server omgeving
- ✕ Fase 2: Implementatie van Intune en migratie NAS naar Wasabi Cloud NAS
- ✕ Fase 3: Migratie data op fileshares naar OneDrive, Teams en SharePoint
- ✕ Fase 4: Vervanging verouderde Windows servers en implementatie RDS

Het is van belang om de eindgebruikers vanaf fase 1 mee te nemen in de migratie. Door de eindgebruikers direct te betrekken is de kans op een positief resultaat groter.

10.2 Beantwoording hoofdvraag

Hoe kan Exite de IT-infrastructuur van een klant optimaliseren en migreren naar de cloud, hoe zal deze migratie moeten verlopen en wat zijn de gevolgen daarvan?

Om de IT-infrastructuur van een klant te optimaliseren en migreren naar de cloud is het van belang om allereerst de huidige omgeving en manier van werken in kaart te brengen. Vervolgens moet onderzocht worden welk type cloudoplossing het beste past bij de klant.

Voor het succes van een optimalisatie en/of cloudmigratie is het essentieel dat de eindgebruikers vanaf het begin betrokken zijn bij de oplossing. Verder is het van belang om eindgebruikers te helpen wennen aan en te leren werken via de cloud en is het belangrijk om de optimalisatie en/of cloudmigratie in behapbare stappen/fases te implementeren.

Cloudmigraties hebben gevolgen voor eindgebruikers en vereisen daarom grondige overwegingen om onvoorspelbare kosten en teleurstellende implementaties te voorkomen. Het juiste moment voor een overstap naar de cloud is wanneer een bedrijf aanzienlijke groei doormaakt en behoefte heeft aan schaalbare diensten. Een kritische evaluatie van systemen en het identificeren van offline toepassingen zijn daarbij essentieel voor een succesvolle migratie. Zonder deze aanpak kunnen de gevolgen groot zijn, zoals een verhoogd risico op datalekken en cyberaanvallen, hoge kosten en instabiliteit van de cloudomgeving.

10.3 Discussie

Het onderzoek beschikt over een aantal beperkingen. Dit betekent niet dat het onderzoek onjuist of onbruikbaar is maar het is van belang om hier rekening mee te houden bij de interpretatie van de resultaten.

Gedurende het onderzoek is niet met de desbetreffende klant gesproken, omdat dit niet mogelijk was. Het kan daardoor voorkomen dat de probleemstelling niet volledig in beeld is gebracht. Omdat de desbetreffende klant niet betrokken kon worden is ervoor gekozen om veel met de customer succes manager van Exite te spreken, omdat diegene nauw betrokken is bij deze desbetreffende klant. Hierdoor is het perspectief en de belangen van de klant alsnog voldoende in kaart gebracht om het onderzoek te kunnen voortzetten.

Om voor specifieke klanten een cloudmigratie uit te voeren is per klant aanvullend onderzoek vereist. In het vervolgonderzoek zal elke applicatie onderzocht moeten worden om na te gaan of deze geschikt is voor de cloud. Verder is het van belang om in samenwerking met deze klanten na te gaan of alle data geschikt is voor OneDrive, Teams/SharePoint. Dit vergt aanvullend onderzoek en daarbij is ook de inspraak van klanten benodigd.

De uitkomst van dit onderzoek kan Exite helpen om haar klanten beter van dienst te zijn bij de migratie van on-premise omgevingen. Om de resultaten van het onderzoek optimaal in te kunnen zetten worden een aantal vervolgstappen aangeraden.

Uit het advies is gebleken dat de omgeving geoptimaliseerd kan worden. Niet alles is geschikt of zinvol om te migreren naar de cloud. Exite kan de omgeving van de desbetreffende klant optimaliseren en deels migreren naar een hybride cloud omgeving. Exite zou een vervolgonderzoek kunnen inzetten bij deze klant om alle applicaties inzichtelijk te maken en te onderzoeken of deze wellicht een SaaS-variant hebben of een soortgelijke SaaS-applicatie, waardoor deze klant wellicht wel klaar is voor een migratie naar een public cloudoplossing.

11 Reflectie

Analyseren (Infra)

Gedurende het scriptieproces heb ik geleerd om te analyseren tegen welk probleem een klant aanloopt en wat een klant op dit moment heeft op het gebied van huidige IT-infrastructuur. Ik heb geleerd om de behoeftes van de klant om te zetten in requirements voor het gericht zoeken naar literatuur en het leveren van input van het ontwerp. Door het continu vragen naar feedback van de bedrijfsbegeleider en andere interne betrokkenen heb ik geleerd om de resultaten te verifiëren, zodat het eindresultaat van voldoende kwaliteit is. Tot slot heb ik geleerd om te analyseren welke producten en diensten Exite levert, om deze verder te onderzoeken en de resultaten daarvan te gebruiken in het ontwerp en advies.

Ontwerpen (Infra)

Gedurende het scriptieproces heb ik geleerd om een gedegen ontwerp op te zetten en de requirements daarin te verwerken. Met behulp van de interviews en het deskresearch in het literatuuronderzoek is generiek gekeken naar technieken, oplossingen en processen om te verwerken in het ontwerp. Het ontwerp is daardoor een combinatie van een maatwerkoplossing voor de klant en een generiek ontwerp om toe te passen bij andere klanten.

Adviseren (Infra)

Gedurende het scriptieproces heb ik geleerd om een gedegen advies op te zetten door onderzoek te doen naar generieke literatuur met betrekking tot cloudmigraties en de betekenis daarvan. In het advies heb ik de generieke resultaten kunnen vertalen naar een passend advies en maatwerkoplossing voor deze klant met concrete vervolgstappen.

12 Bibliografie

Architect, S. (2023, april 6). (K. Hampsink, Interviewer)

Dingemanse, K. (2015, september 8). *Soorten interviews*. Opgehaald van scribbr.nl:
<https://www.scribbr.nl/onderzoeksmethoden/soorten-interviews/>

Exite ICT. (2023). *De X-factor*. Opgehaald van <https://www.exite.com/over-ons/de-x-factor/>

Exite ICT. (2023). *Onze branches*. Opgehaald van Exite ICT: <https://www.exite.com/case/branches/>

Exite ICT. (2023). Waar wij voor staan. *Informatiegids Exite*, p. 31.

Gordon, J. (2021, februari 26). *On Prem To The Cloud: Lift and Shift*. Opgehaald van
<https://devblogs.microsoft.com/devops/on-prem-to-the-cloud-lift-and-shift-ep-2/>

Hancock, J. (2023). *The psychology of human mistakes*. Opgehaald van tessian.com:
<https://www.tessian.com/research/the-psychology-of-human-error/>

Inspark. (2023). *Wat we doen*. Opgehaald van <https://www.inspark.nl/diensten/>

Intercept. (2023). *Azure oplossingen*. Opgehaald van <https://intercept.cloud/nl/azure-oplossingen/>

Jethva, H. (2022, oktober 13). *Remote Desktop Services vs Citrix*. Opgehaald van
<https://cloudinfrastructureservices.co.uk/remote-desktop-services-vs-citrix>

Kai Haverman, E. H. (2022). *Reader Design Research v2.2*. Enschede: Saxion.

Kieft, T. (2022, juni 22). *Succesfactoren bij cloudmigraties*. Opgehaald van
<https://www.kennisportal.com/wp-content/uploads/2022/06/INTO-5-Succesfactoren-bij-Cloud-Migraties.pdf>

Knulst, C. (2022, september 6). *Is een cloudtransitie versnelle wel zo verstandig?* Opgehaald van
<https://www.computable.nl/artikel/blogs/cloud-computing/7407923/5260614/is-een-cloudtransitie-versnellen-wel-zo-verstandig.html>

Kotecha, R. (2022, september 5). *Cloud Migration Strategy – The Ultimate Guide to the 6 R's*.
Opgehaald van <https://www.simform.com/blog/cloud-migration-strategy/>

Krul, A. (2014, april 24). *Hoe voer je een deskresearch uit | Uitleg & voorbeelden*. Opgehaald van
<https://www.scribbr.nl/onderzoeksmethoden/deskresearch/>

Lucidchart. (2023). *Veilige cloud opslag*. Opgehaald van <https://www.lucidchart.com/blog/nl/veilige-cloud-opslag>

- Lucidchart. (2023). *Wat is schaalbaarheid voor systemen en services?* Opgehaald van <https://www.lucidchart.com/blog/nl/wat-is-schaalbaarheid#:~:text=De%20schaalbaarheid%20geeft%20aan%20hoe,in%20je%20hele%20systeem%20steunen.>
- Mendelow, A. L. (1991). Environmental Scanning: The Impact of the Stakeholder Concept. In *Proceedings From the Second International Conference on Information Systems* (pp. 407-418). Cambridge, MA.
- Merkus, J. (2021, september 8). *Semigestructureerd of half-gestructureerd interview | Voorbeeld*. Opgehaald van <https://www.scribbr.nl/onderzoeksmethoden/semigestructureerd-interview/>
- Merkus, J. (2021, juli 15). *Verschil tussen kwalitatief & kwantitatief onderzoek | Voorbeelden*. Opgehaald van <https://www.scribbr.nl/onderzoeksmethoden/kwalitatief-vs-kwantitatief-onderzoek/#:~:text=Kwantitatieve%20dataverzameling%20en%20%2Danalyse%20richt,verschillende%20soorten%20kennis%20te%20verzamelen.>
- Microsoft. (2023, mei 20). *Toepassingen ontwerpen voor schalen*. Opgehaald van <https://learn.microsoft.com/nl-nl/azure/well-architected/scalability/design-scale#use-autoscaling-to-manage-load>
- Microsoft. (2023). *Wat is cloudcomputing?* Opgehaald van [azure.microsoft.com: https://azure.microsoft.com/nl-nl/resources/cloud-computing-dictionary/what-is-cloud-computing/](https://azure.microsoft.com/nl-nl/resources/cloud-computing-dictionary/what-is-cloud-computing/)
- Microsoft. (2023). *Wat is cloudmigratie?* Opgehaald van <https://azure.microsoft.com/nl-nl/resources/cloud-computing-dictionary/what-is-cloud-migration/#definition>
- Microsoft. (2023). *Wat zijn hybride, openbare en privéclouds?* Opgehaald van <https://azure.microsoft.com/nl-nl/resources/cloud-computing-dictionary/what-are-private-public-hybrid-clouds/#benefits>
- Microsoft. (2023). *Windows Server 2012 R2*. Opgehaald van <https://learn.microsoft.com/nl-nl/lifecycle/products/windows-server-2012-r2>
- NIST. (2011, oktober 25). *Final Version of NIST Cloud Computing Definition Published*. Opgehaald van <https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published>
- NIST. (2021, juni). *Digital Identity Guidelines*. Opgehaald van <https://pages.nist.gov/800-63-3/sp800-63b.html>
- PCI. (2023). *Diensten*. Opgehaald van <https://www.pci.nl/diensten/>
- Previder. (2023). *IT diensten*. Opgehaald van <https://previder.nl/diensten>

Projectmanagementsite. (2018, januari 1). *MoSCoW*. Opgehaald van https://projectmanagementsite.nl/moscow/#.Y_yrUD2ZND8

Rapid Circle. (2023). *Diensten*. Opgehaald van <https://www.rapidcircle.com/diensten-1>

Rawworks. (2023). *Deze diensten laten jou sneller en slimmer werken!* Opgehaald van <https://www.rawworks.nl/home/diensten/>

Schop, G. J. (2023). *7S-model*. Opgehaald van managementmodellensite.nl/7s-model-2/

Shanmugiah, R. B. (2022, november 16). *Autoscale*. Opgehaald van <https://docs.citrix.com/en-us/citrix-daas/manage-deployment/autoscale.html>

Success Manager, C. (2023, april 3). (K. Hampsink, Interviewer)

TIBCO. (2023). *What is Immutable Data?* Opgehaald van <https://www.tibco.com/reference-center/what-is-immutable-data#:~:text=Immutable%20data%20is%20a%20piece,when%20new%20data%20is%20available.>

Unica. (2023). *Unica ICT Solutions*. Opgehaald van <https://www.unica.nl/ict-solutions>

Wasabi. (2023). *Wasabi Cliud NAS*. Opgehaald van https://cdn.brandfolder.io/BFD8NB05/at/rb962bhf6bhzc87cbtcj7/Cloud_Nas_Data_Sheet-9-21.pdf

Wasabi. (2023). *Why is Cloud Storage the solution?* Opgehaald van <https://wasabi.com/migrate-premise-storage-cloud/>

13 Bijlagen

13.1 Bijlage A: Stakeholderanalyse

Naar aanleiding van de eerste gesprekken met de opdrachtgever omtrent het onderwerp van het onderzoek, is er een longlist van stakeholders opgesteld. Onderstaande opsomming geeft een weergave van de longlist van stakeholders:

- ✕ Exite ICT
- ✕ Solution Architect(en) Exite
- ✕ Customer Success Manager Exite
- ✕ Manager beheer Exite
- ✕ Security Officer Exite
- ✕ Klant
- ✕ Leveranciers Exite

13.1.1 Categorisering stakeholders

Na de eerste inventarisatie van de stakeholders worden deze in categorieën ingedeeld. Om te kunnen bepalen welke macht en invloed een stakeholder heeft, worden ze ingedeeld op basis van twee categorieën. Deze zijn terug te vinden in onderstaand tabel:

Categorie	Stakeholders
Interne stakeholders	✕ Exite ICT ✕ Solution Architecten Exite ✕ Customer Success Manager Exite ✕ Manager beheer Exite ✕ Security Officer Exite
Externe stakeholders	✕ Klant ✕ Leveranciers Exite

Tabel 24 – Interne- en externe stakeholders

Na het categoriseren van bovenstaande stakeholders, wordt er bekeken welke stakeholders direct of indirect invloed hebben op het project. Dit is belangrijk voor het prioriteren van de stakeholders.

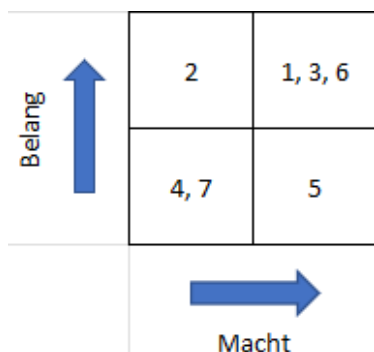
Categorie	Stakeholders
Directe invloed	✕ Exite ICT ✕ Solution Architecten Exite ✕ Customer Success Manager ✕ Leveranciers Exite ✕ Klant
Indirecte invloed	✕ Security Officer Exite ✕ Manager beheer Exite

Tabel 25 – Categorisering stakeholders

13.1.2 Prioritering stakeholders

Om de stakeholders te prioriteren wordt gebruik gemaakt van de Mendelow methodiek (Mendelow, 1991). Deze methodiek wordt gebruikt om de stakeholders te prioriteren op basis van macht en belang. Macht geeft aan welke invloed een stakeholder op het project kan leveren en belang geeft aan in hoeverre een stakeholder direct belang heeft bij het resultaat van het project.

Stakeholders met een hoge score op basis van macht en belang worden automatisch toegevoegd aan de shortlist van stakeholders.



Figuur 16 – Prioritering stakeholders

In onderstaande tabel worden de stakeholders nog eens toegelicht.

Nr.	Stakeholder	Toelichting
1	Exite ICT	Exite heeft als opdrachtgever een hoge macht en groot belang bij dit project. Om dit perspectief te beschrijven is het uitgangspunt gebruikt van een Solution Architect.
2	Solution Architecten Exite	De solution architecten binnen Exite hebben een groot belang bij het project, aangezien zij oplossingen ontwerpen en beheren voor klanten. Ook hebben zij veel macht, zij maken belangrijke afwegingen en adviseren hierin.

3	Customer Success Manager Exite	De customer success managers hebben veel belang bij het project, maar minder macht. Zij zijn verantwoordelijk om de eisen en wensen van de klant goed in kaart te brengen en willen de klant tevreden stellen.
4	Manager Beheer Exite	De manager beheer heeft zowel minder belang als minder macht bij het project. Hij/zij voert geen directe werkzaamheden uit bij klanten.
5	Security Officer Exite	De security officer heeft wat minder belang en veel macht bij het project. Hij/zij is verantwoordelijk voor de beveiliging van zowel nieuwe als bestaande oplossingen.
6	Klant	De klant heeft een groot belang bij het project. Zij gaan immers gebruik maken van de oplossing. Omdat het externe stakeholders zijn hebben zij geen directe invloed.
7	Leveranciers Exite	Leveranciers hebben geen directe macht bij het project. Exite is afhankelijk van leveranciers, maar kan kiezen voor een andere leverancier. Leveranciers hebben geen belang bij het resultaat van het project.

Tabel 26 – Stakeholders

13.1.3 Stakeholderselectie probleemanalyse

Stakeholders die een grote mate van macht of invloed hebben op het project worden opgenomen in de shortlist van stakeholders die betrokken worden bij het probleem. Stakeholders met weinig macht of invloed worden niet in die lijst opgenomen, omdat zij onvoldoende invloed hebben op of belang hebben bij het uiteindelijke resultaat.

- ✕ Opdrachtgever (Solution Architect)
- ✕ Customer Success Manager
- ✕ Security Officer
- ✕ Klant

13.1.4 Stakeholderselectie behoefteanalyse

Om een zo volledig mogelijke lijst van requirements op te stellen, worden de behoeften vanuit verschillende perspectieven bekeken. Hiervoor is de stakeholderanalyse, zoals beschreven in de bijlage, geraadpleegd. Figuur **XX** geeft aan welke stakeholders een hoog of laag belang hebben bij de uitkomst en welke stakeholders macht hebben op het onderzoek. Aangezien de behoefte voortkomt uit de stakeholders met een hoog belang, wordt de behoefteanalyse uitgevoerd vanuit het perspectief van deze stakeholders.

De volgende stakeholders hebben op basis van de stakeholderanalyse een hoog belang bij de uitkomst van het onderzoek:

- ✕ Solution Architecten
- ✕ Security Officer
- ✕ Klant

13.1.5 Stakeholderselectie contextanalyse

Voor het uitvoeren van een interne analyse, wordt er alleen met interne stakeholders gesproken. Deze stakeholders kunnen een goed beeld geven van de organisatie. Het gaat om de volgende interne stakeholders:

- ✕ Opdrachtgever (Solution Architect)
- ✕ Customer Success Manager
- ✕ Security Officer
- ✕ Manager Beheer

13.2 Bijlage B: Interviews

13.2.1 Methodiek

Om zoveel mogelijk informatie te verkrijgen van de belanghebbenden worden er semigestructureerde interviews gehouden. Semigestructureerde interviews worden ook wel kwalitatieve interviews of diepte-interviews genoemd. Hierbij gebruik je een algemeen interviewschema met vooropgestelde, wat algemener geformuleerde, vragen, maar je mag hier wel van afwijken. Zo kun je bijvoorbeeld doorvragen als je respondent iets interessants zegt of als je niet helemaal begrijpt wat diegene bedoelt. Hiermee verkrijg je meer en gedetailleerde informatie, wat in kwalitatief onderzoek vaak het doel is. (Dingemanse, 2015)

13.2.2 Resultaten

Interview vragen

Vragen solution architect tevens opdrachtgever:

- ✕ Welke verschillende methodes heb je voor migratietrajecten?
Lift & shift of bijvoorbeeld het bestaande (applicatie)landschap te verSaaSen, het beheer valt daardoor weg. Dit heeft over het algemeen wel meer impact. Met lift & shift verplaats je de huidige omgeving in principe van bijvoorbeeld een private cloud naar bijvoorbeeld Azure. Wat zijn de kritische succesfactoren?
Het is belangrijk om de verwachting van de klant van te voren duidelijk te hebben om daaraan te voldoen en/of te overtreffen. Ook is het belangrijk om binnen de tijd en budget te blijven. Je moet de juiste mensen koppelen, denk aan communicatie en de impact op de core business te beperken.
- ✕ Wat zijn de voordelen van het migreren naar de cloud?
In Azure heb je overal toegang toe als je zelf een administrator bent. Je kan als klant ook kiezen om (een deel) zelf te beheren. In de private cloud kan dat bijvoorbeeld niet.
- ✕ Wat zijn de voordelen van het migreren naar de cloud?
In Azure zijn zaken beter op orde qua beveiliging dan bij Exite/Equinix/Fundaments. In Azure kan je ook resources vast zetten voor een bepaalde periode (1 jaar, 2 jaar etc.), daarmee krijg je korting tot 70% op de resources, dit heet Azure reserved instances. Hetzelfde geldt ook voor Azure virtual desktop. Je zou er ook voor kunnen kiezen om servers op standaard kantoor tijden aan te zetten en deze (Citrix)servers buiten kantoor tijden weer uit te zetten. Er is al een klant die dat op die manier gebruikt. Die Citrix servers worden ook automatisch op en af geschaald. Er wordt wel vaker gekozen voor Azure reserved instances dan voor het scheduled aan en uitschakelen. Je kunt ook gebruik maken van Azure saving plans. Dit kan je gebruiken op andere resources dan bijvoorbeeld virtuele machines.
- ✕ Welke beveiligingsmaatregelen moet je nemen voor, tijdens en na het migratieproces?
Vanuit Exite zijn er wel standaarden bij het inrichten van een moderne werkplek, bijvoorbeeld het verplichten van licentie Azure p1 of p2 met standaard MFA en standaard policy's. Als een klant Intune afneemt hebben we daar ook een standaard baseline voor. Denk daarbij aan het verplichten van bitlocker en het afdwingen van Windows Hello.
- ✕ Hoe minimaliseer je de verstoring van bedrijfsprocessen tijdens de migratie?

Wij proberen altijd de impact te beperken tot het minimum door alles in goed overleg te doen met de klant.

- ✕ Hoe zorg je ervoor dat de applicaties compatibel zijn met de cloud?

Legacy applicaties kunnen we aanbieden middels Azure virtual desktop. Hiervoor heb je alleen een computer met nodig welke een RDP-verbinding kan opzetten naar de Azure virtual desktop. Bij voorkeur nemen we de server kant van de applicatie ook op in Azure. Zo heb je geen extra VPN-verbinding nodig tussen client en server, waardoor je ook geen extra latency hebt. Hiervoor heb je wel vaak de leverancier nodig. De leverancier voert die migratie uit, omdat wij geen applicatie inhoudelijke kennis hebben van iedere specifieke applicatie.

Vragen customer succes manager/sales:

- ✕ Kan je wat vertellen over je functie en verantwoordelijkheden bij Exite?

Ik ben customer success manager, zoals dat heet bij Exite. Je kunt dat vergelijken met sales consultant en accountmanager. Mijn functie houdt eigenlijk in om nieuwe klanten aan ons te binden, relatiebeheer en het uitbreiden van klanten. Dit doe ik door advies te geven in keuzes die ze hebben qua beveiliging, migratietrajecten en een nieuwe moderne werkplek was dan ook weer aansluit bij beheercontracten. Ik ben verantwoordelijk voor het binnenhalen van klanten en het succes te behouden bij klanten. Dit doe ik ook vanuit een commerciële doelstelling.

- ✕ Wat zijn belangrijke succesfactoren, wanneer jullie een oplossing aanbieden?

Ik vind het belangrijk dat je begint met kijken in welke situatie zit de klant nu, hoe werken ze nu en sluit dat aan bij wat ze willen. Vanuit daar kijken wij hoe je ze het beste kunt faciliteren. Wanneer je een plan bedenkt wat niet doelt op de juiste zaken gaat het vanaf daar al mis. Wat ook erg belangrijk is, is om voortdurend nadenken hoe je de adoptie gaat aanpakken, een stukje verandermanagement.

- ✕ Wat zijn organisatorische gevolgen om rekening mee te houden voor een klant?

IT wordt steeds functioneler, het is belangrijk om eindgebruikers (key users) mee te nemen in de gehele verandering/migratie. Daar begint de adoptie al mee. Om dat goed te faciliteren ga je naar een pilot fase om het te testen. Vervolgens komt de livegang/migratie met bijbehorende nazorg.

- ✕ Welke diensten/mogelijkheden bieden jullie aan?

In principe zijn de smaakjes wel bekend, het is afhankelijk van de huidige omgeving wat er mogelijk is. We hebben standaard oplossingen vanuit Microsoft 365 gedachte, remote desktop oplossingen met verschillende keuzes, always-on-VPN constructies en meerdere standaard oplossingen met dienstverlening en migratieplannen. Welk scenario het wordt is ook afhankelijk van de klant en de situatie. Heeft de klant bijvoorbeeld een eigen IT-afdeling of doen wij alles, dat is een stuk maatwerk wat er altijd in zit. Het is nooit plug and play.

- ✕ Wat zou jou belang zijn bij het uitvoeren van het project voor de klant?

Als je naar een moderne werkplek gaat krijg je als eindgebruiker veel meer mogelijkheden om je werk op een prettige manier in te richten, je kan lokaal gaan werken, waardoor de performance beter is. Ten tweede kan je de mogelijkheden van Microsoft 365 makkelijker benutten. Ook is het vaak beter werken in plaats van een remote desktop omgeving. Vanuit een Microsoft 365 omgeving kun je veel meer functies gaan gebruiken waardoor je je werk nog beter kunt organiseren.

- ✕ Wat belangrijke zaken op het gebied van beveiliging bij klanten?

Beveiliging is altijd een van de belangrijkste punten, maar het zit in een soort balans. Hoe veiliger je het maakt hoe beperkter alles ook wordt voor de eindgebruiker, maar als je alles kunt heb je weer geen grip op de beveiliging. Beveiliging moet als een soort rode draad door je migratieplan lopen, door alle facetten heen, heel veel kan je afdwingen en voorkomen maar er zit ook opleiding en training achter in de vorm van een security awareness training. Wat we vaak doen binnen zorgklanten is een werkplek op basis van een 7510 normering, daarmee heb je bepaalde zaken standaard ingericht, zoals Intune en Azure, wat je waar wel en waar niet mag openen, zo waarborgen we de beveiliging. Die trainingen worden door de security consultant uitgevoerd en de nulmetingen worden ook door diegene gedaan. Zo kan er bepaald worden hoe omgevingen beter beveiligd kunnen worden.

- ✕ Wat zijn de huidige knelpunten op het gebied van beveiliging bij deze specifieke klant?

De twee grootste knelpunten zijn op dit moment dat ze een legacy omgeving hebben waar ze moeilijk van af kunnen. Ze hebben een Citrixomgeving waar weinig van de Microsoft 365 facetten benut kunnen worden. Ze werken ook nog deels lokaal, dus eigenlijk werken ze vanuit twee omgevingen. Hun data staat deels in Teams/SharePoint/OneDrive en deels op netwerkshares. Eigenlijk is hun omgeving gedeeltelijk getransformeerd de laatste jaren, maar er zit geen goed plan onder hoe ze nu het beste en makkelijker kunnen gaan werken. Ze kunnen er veel meer uithalen door een goede basis in te richten om de mensen er ook goed mee te kunnen laten werken. Vanuit beveiliging staat data nu op verschillende plekken en Intune is niet voldoende ingericht om de beveiliging op werkplekken 100% te kunnen afdichten. Als je buiten die Citrix omgeving wilt gaan werken is het goed om de werkplekken en het beheer goed onder controle te hebben, zodat je daarmee al een stuk van je beveiliging kunt inregelen. Dat is wel belangrijk knelpunt op dit moment.
- ✕ Hoe ziet de huidige infrastructuur eruit van deze klant?

Ze hebben een aantal applicaties al in de cloud draaien. Zij zijn reeds overgestapt naar Dynamics, maar dat is een maatwerk implementatie geweest en heeft nog twee servers nodig. Daarmee ben je nog afhankelijk, deze servers draaien al wel in het datacenter. Ze hebben ook nog een oude applicatie server voor SAP, deze draait ook in het datacenter, maar dat is meer archief. Wordt gebruikt voor het ophalen van info en er is daarop geen productieomgeving naar de klant toe. Ook hebben ze fileservers waar data op staat die engineers gebruiken en hebben ze een monitoring oplossing voor turbines. De software daarvan draait in datacenter. Dynamics is dus al deels SaaS, maar heeft dus nog wel twee servers nodig, voor printen of warehouse of iets dergelijks, dit weten ze zelf ook niet zo goed. Een aantal engineers hebben lokale applicaties op de werkplekken staan voor het uitmeten van de turbines, deze staan lokaal op de werkstations en daar zijn allerlei verschillende versies van die ze gebruiken, deze versies zijn weer afhankelijk van hoe oud een turbine is bij wijze van spreken. Het is dus echt maatwerk per turbine/werkstation. De installatie doen ze zelf van die applicaties.
- ✕ Hoe zie jij een oplossing in deze probleemstelling?

In principe is alles wat een server nodig heeft al in het datacenter opgenomen van fundamentals, private cloud. Het is de keuze voor hun om die servers wel of niet naar bijvoorbeeld Azure te brengen. Ze zullen de server infrastructuur wel nodig blijven houden om hun omgeving te kunnen blijven faciliteren. In Azure heb je wel als voordeel dat je archiefapplicaties uit kunt zetten en alleen aan kunt zetten wanneer nodig, wat weer kosten kan besparen. Alles wat in het

datacenter staat kan niet als SaaS oplossing aangeboden worden. SAP is gewoon archief en daar gebeurt niet veel mee, die servers voor Dynamics is de vraag wat daar mee kan en of ze nodig zijn, maar waarschijnlijk wel. De monitoring oplossing is zo specifiek die waarschijnlijk ook een server nodig blijft houden, waar die staat (private cloud of Azure) maakt niet uit. Alle data die daar uit komt gaat momenteel naar een server welke daar lokaal staat en wordt gebackuppeld naar een NAS bij hun op locatie. Deze grote hoeveelheden data kan vast naar de cloud maar of dat kosten efficiënt is, is de vraag. Het belangrijkste is om de omgeving zo makkelijk mogelijk te maken en een goed dataplan hebben, waarin staat waar welke data staat, om te voorkomen dat niet op 10 plekken dezelfde data staat. De huidige Intune omgeving moet strakker worden ingericht, dit is wel belangrijk voor borgen van beveiliging. Om kosten te besparen kan gedacht worden aan bijvoorbeeld Citrix uit te faseren, en er eventueel voor kiezen om naar Azure heen te brengen zodat je servers kunnen uit zetten wanneer je ze niet nodig hebt.

Vragen solution architect/consultant:

- ✕ Kan je wat vertellen over je functie en verantwoordelijkheden bij Exite?
Ik ben vaak al bij het presales traject betrokken en krijg dan onder andere informatie van de Customer Success Manager/Sales. Als het dan te technisch wordt haak ik aan. Ik probeer dan zo goed mogelijk een technisch plaatje te krijgen van de eisen en wensen van de klant. Ik probeer dat samen met de Customer Success Manager zo goed mogelijk te laten landen bij de klant.
- ✕ Hoe ziet de huidige omgeving eruit bij Opra?
Bij de klant Opra hebben wij bijvoorbeeld 2 voorstellen gedaan. Eerst een stukje optimalisatie van de huidige omgeving in de private cloud bij Fundaments. Dit is momenteel een redelijke traditionele manier, denk hierbij aan Citrix, Office365 en verschillende applicatie- en fileservers. De manier van werken bij hun is redelijk versnipperd, de ene persoon werkt op een laptop, anderen maken gebruik van de Citrix omgeving. Ze hebben ook een traditionele Dynamics omgeving, een client-server model. Bij het onderzoeken naar een nieuw ERP pakket zal er eerst gekeken moeten worden naar een SaaS dienst. Reden dat dat niet mogelijk is kan zijn dat ze veel maatwerk hebben die niet in de SaaS versie van Dynamics zit. Het nadeel is dat ze dat zelf ook niet zo goed weten. Het zou wel de weg vrij maken om de rest ook te verSaaS en/of volledig naar Azure te gaan. Het tweede voorstel wat we hebben gedaan is een upgrade van de huidige omgeving. Het overgaan naar volledig werken vanuit Azure. Dit houdt in dat een aantal machines worden opgenomen in Azure, werkplekken beheerd worden vanuit Intune. Deze twee voorstellen hebben we naast elkaar gelegd met de voor- en nadelen en de kosten. Wat we eerder gedaan hebben is met eind gebruikers (key users) om tafel gaan. We vragen dan zoveel mogelijk informatie uit, zoals waar slaan ze de data op, waar halen ze die data vandaan en wat zijn de huidige struikelblokken.
- ✕ Hoe bepaal je welke applicaties geschikt zijn voor de cloud en welke niet?
Dan kijken we naar waar slaan ze verschillende soorten data op, is dat bijvoorbeeld op een database, gaat het om platte bestanden (documenten), want dan moet je gaan kijken of die bestanden naar Teams en SharePoint zouden kunnen worden gemigreerd. Het nadeel is dat 9 van de 10 keer dat niet kan. Dat werkt bijvoorbeeld goed met het Office pakket, maar al het andere wordt al lastig. Bij een andere klant loopt nu een migratie naar Teams/SharePoint, daar werken ze niet met Microsoft project maar een alternatief daarvan. Als het Microsoft was geweest had het goed gekund. Het samenwerken in bestanden is nu niet mogelijk en het is niet

makkelijk te openen vanuit Teams/SharePoint. Opra heeft dit ook, specifieke pakketten, bestandsformaten die niet worden ondersteund door Teams/SharePoint. Een alternatief is mappen synchroniseren door middel van netwerkshares, maar dat brengt ook uitdagingen met zich mee, niet samenwerken in documenten bijvoorbeeld.

- ✕ Hoe bepaal je de juiste cloudprovider voor een klant?
Wij zijn een Microsoft gold partner. In principe proberen wij zoveel mogelijk Microsoft oplossingen te implementeren. Maar alternatieven sluiten wij zeker niet uit, als dat beter is.
- ✕ Welke beveiligingsmaatregelen moet je nemen voor en/of tijdens het migratieproces?
Normaal doen we op het moment dat alle data verplaatst wordt naar Teams/SharePoint een stukje adoptie. Dat houdt in dat er een workshop aan vast zit. Ook gaan we in gesprek met key users over hoe kunnen we het beste inrichten, wie moet waar toegang tot hebben, mogen bepaalde mappen wel of niet worden gedeeld met externen, afstemming is erg belangrijk. Voorheen deden we hetzelfde met fileservers en shares, alleen nu zijn er meer mogelijkheden. Zit meer uitvraag aan vast, met bijvoorbeeld RBAC. We proberen altijd zoveel mogelijk gebruik te maken van functieprofielen in het geven van rechten.
- ✕ Hoe verminder je downtime tijdens het migratieproces?
Meestal pakken we daar een weekend voor in overleg met de klant, voor data migratie gebruiken we de SharePoint migration tool, dat is gratis tool van Microsoft. Voorafgaand de migratie weten we al welk mapje naar welke Teams map/kanaal moet. Voor die tijd wordt de Teams omgeving ook al aangemaakt en ingericht. Door middel van een CSV-bestand wordt dan alles overgezet. Hierin staat welk mapje naar welke nieuwe locatie moet. Meestal lukt zo'n migratie met een nacht en een dag, maar is ook afhankelijk van hoeveelheid data.
- ✕ Hoe doe je dat als het gaat om een 24/7 business?
Dan hebben we al snel een uitdaging, want er komt gewoon een cutover moment. Waarin je een keer om zal moeten. Gelukkig zijn we tot nu toe nog nooit in een situatie gekomen waarin het echt niet kon. Er zijn wel momenten waarin het wel kan. Eer moet ook van te voren getest worden, hoelang duurt dan zo'n migratie, maar dat zal altijd een ruwe schatting zijn.
- ✕ Hoe zorgt je ervoor dat de applicaties en gegevens beschikbaar blijven tijdens de migratie?
Citrix servers zijn redelijk statisch, daar verandert weinig aan. Deze kan je wel migreren naar Azure, dan maak je er een kopie van, werk je aan de kopie, zodat deze helemaal klaar is voor Azure. Zo is het redelijk makkelijk om te zetten. Bij de overgang zet je de toegang tot de oude Citrix omgeving uit, en de toegang tot de nieuwe in Azure zet je aan. Vervolgens moet je zorgen dat de juiste mensen de juiste koppelingen hebben naar de virtuele desktop in Azure. De overgang plan je ook gewoon in zoals een bij een datamigratie. Altijd zo goed mogelijk voorbereiden, zodat zoveel mogelijk al op de juiste plek staat, vervolgens kan je dan in het weekend/ tijdens het migratiemoment alleen de laatste zaken nog overbrengen en de toegang omzetten. Oude shares dicht zetten en toegang tot de juiste Teams mappen en SharePoint mappen openzetten.
- ✕ Hoe zorg je ervoor dat de applicaties compatibel zijn met de cloud?
Dat een applicatie echt niet geschikt is kom je vrijwel weinig tegen. Een statische applicatie kan je naar de cloud brengen door bijvoorbeeld een virtuele desktop oplossing aan te beiden. En dat het dan een traditionele RDS omgeving is of Azure virtual desktop is maakt niet uit. Zo kan je elke oude traditionele applicatie wel laten landen. Het voordeel van Azure virtual desktop is dat je servers kunt uitzetten, dan betaal je er ook niet voor. In een private cloud omgeving betaal je altijd voor de resources, of ze nu aan of uit staan.

- ✕ Hoe zorg je ervoor dat de cloudoplossing flexibel is en kan worden aangepast aan veranderende behoeften van de klant?

Als je naar Azure migreert, kan je redelijk makkelijk resources aan en uit zetten. Als je resources uitzet welke niet meer gebruikt worden, betaal je alleen nog maar voor de storage. Mocht het toch nodig zijn kan je hem ook weer aanzetten. Bij Fundaments, onze private cloud, betaal je altijd voor de resources. Bij Azure alleen als deze aanstaat (op storage na). Op dit moment is Azure dan ook goedkoper dan een private cloud oplossing.

- ✕ Zou dit (migratie naar Azure) dan een goede oplossing zijn voor deze specifieke klant?

Ja, dat zou goed kunnen. Archiefdata is in Azure wel wat duurder ten opzichte van de andere oplossingen. Maar we hebben ook een andere dienst, Wasabi, die je daarvoor kunt gebruiken. Wasabi is ook een cloud oplossing zoals Azure en is kosten technisch heel aantrekkelijk. Bij Wasabi kun je data immutable maken. Zo kunnen er geen wijzigingen op die data plaatsvinden en beveilig je deze data ook meteen tegen ransomware/versleuteling van de data. Wasabi is gevestigd in Amazon datacentra, met ook datacentra in West-Europa. Deze Wasabi cloud NAS oplossing maakt gebruik van slimme techniek, het werkt het zelfde als de bekende OneDrive client. Als je bestanden minder gebruikt worden deze weggeschreven naar de cloud en gebruik je deze bestanden weer, dan haalt de client het weer op. De data wordt aangeboden op basis van een netwerkshare en je kunt veel zelf instellen, zoals retentiepolicy's. Het ophalen van de data van de cloud naar de client gaat enorm snel, je merkt hier als gebruiker vrijwel niets van. Mocht je echt bestanden van bijv. IGB ophalen kan het wel iets langer duren natuurlijk.

- ✕ Hoe zorg je ervoor dat de cloudoplossing voldoende schaalbaar is?

In Azure is het erg gemakkelijk servers op en af te schalen en aan en uit te zetten. Hiermee is de omgeving erg flexibel.

- ✕ Wat zou jou belang zijn bij het uitvoeren van het project voor de klant?

Benader elke oplossing vanuit de eindgebruiker, je kan de meest fantastische en technische oplossingen bedenken, maar de eindgebruiker moet er wel fatsoenlijk mee kunnen werken. Met deze nieuwe manier van werken kan wel met stukje training aan vast zitten, daar houden we altijd rekening mee, dit gebeurt in het adoptieproces. Het is belangrijk om key users altijd mee te nemen. Zij weten wat er speelt en hoe bedrijfsprocessen in elkaar steken waar wij rekening mee moeten houden.

- ✕ Wat zijn de huidige knelpunten bij deze klant?

Ik denk dat het grootste knelpunt momenteel geld is. Ze zijn onlangs failliet gegaan en nu overgenomen door een investeringsmaatschappij. Er gaat veel veranderen, ze hebben nu een eigen IT omgeving (in onze private cloud), maar het kan zo zijn dat ze worden geïntegreerd bij een andere partij. Ze weten het zelf ook nog niet zo goed, ze gaan er vanuit dat ze in principe doorgaan zoals ze altijd hebben gedaan. Het is voor hun dan ook prima te migreren naar bijvoorbeeld Azure en Teams/SharePoint. Of ze daadwerkelijk gaan tekenen voor de opdracht zal dan blijken.

Vragen business consultant & security officer:

- ✕ Kan je wat vertellen over je functie en verantwoordelijkheden bij Exite?

Ik ben verantwoordelijk voor de interne informatiebeveiliging bij Exite, klantvragen die er zijn vanuit bijvoorbeeld de solution architecten en bewaken van de zaken omtrent de certificeringen die we hebben. Met name iso27001 is erg belangrijk voor ons. Op het moment dat er vragen zijn

omtrent security, dan kloppen collega's bij mij aan om eens mee te denken over wat nou een veilige manier is om bepaalde dingen te doen. Dat kan zijn het opstellen van een nieuwe infrastructuur met security controls tot het veilig versturen van een e-mail, het is dus heel breed.

- ✕ Wat moet er gedaan worden om ervoor te zorgen dat de beveiliging in een cloudomgeving voldoende is?

Wij hebben wel een bepaalde project aanpak gedefinieerd, maar engineers richten vanuit hun zelf vaak al bepaalde zaken standaard in. We hebben ook een aantal security baselines gedefinieerd, deze worden momenteel ook aan het licht gehouden in een ander afstudeerproject, daar moeten we als bedrijf zijnde nog wel in professionaliseren.

- ✕ Wat zijn beveiligingsknelpunten bij on-premise omgevingen?

Zeker bij klanten met lokale infrastructuur zijn er knelpunten. Je moet er dan wel voor zorgen dat netwerksegmentatie goed ingericht is, back-ups buiten het interne netwerk opslaan, ervoor zorgen dat je nooit vanuit je interne netwerk bij managementsservers of bij een back-up kan komen. Je ziet dat dat soort klanten wel gevoelig zijn voor gijzelsoftware aanvallen, daar moet je wel bepaalde security controls ingericht hebben, zoals goede firewall regels.

- ✕ Geldt dat ook voor omgevingen welke in de private cloud draaien?

Wanneer je in de private cloud draait, zijn er al een aantal zaken welke wel goed ingericht zijn vanuit de private cloud hosting zelf, denk aan veilige back-ups en het scheiden van netwerken. Deze maatregelen zijn daar al sneller ingebouwd dan wanneer je echt op locatie nog zaken hebt draaien.

- ✕ Als je zou kijken naar de archiefdata, welke ze nog op locatie hebben staan. Waar moet ik rekening mee houden?

Je moet dan gaan kijken of bovenstaande security controls ingericht. Als een aanvaller binnenkomt, kan diegene dan bij die data komen met bijvoorbeeld de rechten van een medewerker of zijn er bepaalde kwetsbaarheden, waardoor ze gemakkelijk rechten kunnen krijgen op admin niveau. Ook moet je kijken naar wat voor een soort data dat dan is. Gaat het bedrijfsgevoelige data en/of persoonsdata, dan is het vele malen belangrijker dan wanneer dat niet het geval is.

- ✕ Hoe zorg je ervoor dat de data veilig is tijdens de migratie?

Je moet ervoor zorgen dat data over een beveiligde lijn wordt getrokken, zodat daar niemand tussenin kan gaan staan. Migraties direct naar de cloud middels zakelijke internetlijnen gaat eigenlijk altijd wel goed. Je moet wel goed kijken naar welk platform gaan we dat op landen, is dat platform goed beveiligd en wie moet er toegang hebben en wie niet. Dit moet je ook vergelijken met hoe is dat nu en hoe zou dat beter kunnen.

- ✕ Welke beveiligingsmaatregelen moet je nemen voor en/of tijdens het migratieproces?

In principe geldt hetzelfde als bovenstaande, ik heb nog nooit meegemaakt dat data tijdens een migratie verloren is gegaan. Het blijft wel belangrijk om te kijken of het qua security ook een verbetering is ten opzichte van de huidige omgeving?

- ✕ Hoe zorg je ervoor dat de cloudoplossing voldoet aan de beveiligings- en compliance-eisen?

Het is belangrijk om te controleren of leveranciers voldoen aan de certificeringen, waaronder de 27001, die specifiek is ontworpen voor hoe Exite omgaat met informatiebeveiliging. Het is echter belangrijk om op te merken dat deze certificering niet aan klanten wordt afgegeven en niet betekent dat alles wat we doen in jouw omgeving direct getoetst kan worden aan de 270001. In

plaats daarvan gaat het om de interne processen die we gebruiken om de informatie te beveiligen. Dit wordt tijdens audits ook niet specifiek gecontroleerd.

We voeren wel bepaalde controles uit voor systemen, zoals het controleren van het type leverancier, waar de gegevens worden opgeslagen (bijvoorbeeld alleen in West-Europa), de certificeringen van de leverancier die we kunnen opvragen, of de gegevens zijn versleuteld en of de verbinding veilig is. Dit zijn allemaal belangrijke aspecten die we in overweging nemen bij het selecteren van leveranciers en het samenstellen van dienstenpakketten voor onze klanten.

- ✕ Wat zou jou belang zijn bij het uitvoeren van het project voor de klant?

Dat hangt af van de omvang van de scope. Als we bijvoorbeeld besluiten om een 1-op-1 migratie naar Azure uit te voeren, dan is de standaardbeveiliging van Azure al voldoende. Echter, als de klant te maken heeft met veel persoonlijke gegevens, dan moeten we nadenken over het versleutelen van de databases en extra technische controles invoeren om een extra beveiligingslaag te creëren.

We moeten ook kijken naar wie er toegang krijgt tot de Azure-omgeving en de databases. Is het de klant zelf of hebben andere partijen toegang? En is er voldoende beveiliging ingebouwd, zoals MFA? Het is belangrijk om alle logische stappen kritisch tegen het licht te houden en te controleren of deze veilig zijn.

Ook de back-up is een belangrijk onderdeel van de beveiliging. Waar wordt de back-up opgeslagen, binnen Azure of op een ander platform? En hebben de personen die toegang hebben tot de Azure-omgeving hoge rechten om bij de back-up te komen? Dit zijn allemaal zaken waar we aan moeten denken bij het opzetten van een veilige omgeving en waar we over kunnen meedenken op het gebied van security.

- ✕ Vanuit de solution architect heb ik gehoord over een nieuwe dienst voor het opslaan van data, Wasabi. Wordt dit al veel gebruikt of staat dit nog in de kinderschoenen?

Dat is inderdaad een nieuwe dienst, deze bieden we steeds vaker aan bij onze klanten.

- ✕ Is Wasabi dan een onderdeel van Microsoft of een losstaand platform?

Dit platform staat volledig op zichzelf en is een Amerikaanse partij. Maar het heeft dataopslagmogelijkheden in Europese datacenters. Bij de beoordeling van dit platform op het gebied van security hebben we gekeken naar hoe ze dit hebben ingericht. Hieruit bleek dat ze serieus bezig zijn met beveiliging en dat we erop kunnen vertrouwen.

Het is in feite een grote archiefbak waar je data kunt opslaan en op basis van bepaalde instellingen kun je aangeven of de data wel of niet gemakkelijk kan worden teruggehaald. Je kunt ook aangeven of iemand anders er wel of niet bij mag komen. Als je het als back-up gebruikt, kun je aangeven wie toegang heeft om de gegevens terug te zetten.

13.3 Bijlage C: Behoeftanalyse

13.3.1 Methodiek requirementsanalyse

Er is een requirementsanalyse opgesteld om de eisen en wensen van de stakeholders in kaart te brengen. De requirements zijn in eerste instantie onderverdeeld in drie onderwerpen en vervolgens geprioriteerd in verschillende categorieën met behulp van de MoSCoW-methode (Projectmanagementsite, 2018).

De requirements worden eerst onderverdeeld in drie categorieën, namelijk Business-, User- en System requirements.

- ✖ Business requirements omvatten het doel van het project en beantwoorden de vraag waarom het systeem ontwikkeld wordt.
- ✖ User requirements brengen de eisen en wensen van de gebruiker in kaart en beantwoorden de vraag wat er ontwikkeld zal worden in het systeem.
- ✖ System requirements beschrijven de benodigdheden voor het systeem en beantwoorden de vraag hoe het systeem gebouwd moet worden.

Na bovenstaande categorisering worden de requirements geprioriteerd met behulp van de MoSCoW-methodiek, daarmee worden deze gerangschikt op hun belang voor de opdracht.

- ✖ Must have. Een must have is een harde eis waaraan niet te tornen valt. Hier moet de oplossing gewoonweg aan voldoen. Als het beoogde resultaat niet wordt behaald, voldoet het projectresultaat niet aan de eisen en is de oplevering of het project mislukt.
- ✖ Should have. Een should have is ook een eis, maar geen keiharde. Hieraan moet eigenlijk ook aan voldaan worden, maar er is wel enige speling: misschien mag het resultaat enigszins afwijken, is er een alternatieve oplossing mogelijk, of kan de eis bij een volgende oplevering meenemen.
- ✖ Could have. Een could have is geen eis, maar een wens. De inspanning heeft meerwaarde en het is zeker nuttig de wens in te vullen, maar dit is niet noodzakelijk. Could have's zijn zaken waar tijd aan besteed kan worden als aan de must en should have's is voldaan en er nog wat tijd en middelen over zijn.
- ✖ Won't have. Een won't have is een eis of wens, waarvan is afgesproken dat deze – in ieder geval in de huidige sprint/oplevering – niet binnen de scope valt. Het is dus niet zo, dat het leuk zou zijn als deze eis of wens wordt ingevuld. Integendeel: er mag aan een won't have geen tijd en resources besteed worden, want dit heeft namelijk geen toegevoegde waarde of gaat ten koste van belangrijkere requirements.

Ook wordt er onderscheid gemaakt tussen functional en non-functional requirements.

- ✕ Functional requirements voegen functies toe aan het systeem en worden door gebruikers gebruikt.
- ✕ Non-functional requirements hebben geen betrekking op de functionaliteit van een requirement, maar geven aan hoe het systeem moet presteren.

Ten slotte worden de requirements aan elkaar gekoppeld door middel van relaties tussen deze requirements, die worden gelegd door middel van genereren en realiseren:

- ✕ Bij genereren wordt bepaald welke requirement wordt gegenereerd. Business requirements genereren User requirements en User requirements genereren System requirements.
- ✕ Bij realiseren wordt bepaald welke requirement wordt gerealiseerd. System requirements realiseren User requirements en User requirements realiseren Business requirements.

13.4 Bijlage D: 7S-model

13.4.1 Methodiek

Om een goed beeld van Exite te krijgen is gebruik gemaakt van het 7-S model van McKinsey (Schop, 2023). Om een interne analyse te maken van Exite ICT wordt het 7-S model van McKinsey gebruikt. Dit model beschrijft zeven aspecten van een organisatie die onderling samenhangen en samen bepalend zijn voor het succes van de organisatie.

13.4.2 Resultaten

Shared Values (Missie & Visie)

Exite ICT is een IT-bedrijf dat diensten aanbiedt op het gebied van IT-infrastructuur, cloudoplossingen, cybersecurity en managed services. Shared Values (Missie & Visie)

Om kort en bondig het bestaansrecht van Exite duidelijk te maken – en daarmee te weten waar we dagelijks voor werken – hebben we een missie. Deze vertelt zo helder mogelijk wat ons drijft:

- Wij prikkelen mens en organisatie om met slimme inzet van ICT hun maximale potentieel te benutten en impact te maken op de wereld van morgen.

We kijken niet alleen naar vandaag, we kijken ook naar de toekomst. Dit is de visie van Exite:

- In de **digitale revolutie** brengen wij **mens en technologie** op succesvolle wijze in **balans**, waardoor we organisaties in staat stellen om hun **ongekende vermogens** te realiseren en **het beste uit zichzelf** te halen. (Exite ICT, 2023)

Strategie

Exite prikkelt mens en organisatie om met slimme inzet van ICT hun maximale potentieel te benutten en impact te maken op de wereld van morgen. Op strategisch niveau brengen ze de business verder door samen slimme ICT-strategieën te ontwikkelen die de organisatie succesvol digitaal laat transformeren. In deze zogenaamde co-creatie komen ze tot betere keuzes. Keuzes die zich altijd terugbetalen. Keuzes die de organisatie voorop laat lopen. (Exite ICT, 2023)

Structuur

Exite ICT heeft een platte organisatiestructuur met korte lijnen tussen medewerkers. Dit past bij de flexibele en agile manier van werken die Exite ICT hanteert. Het stelt hen in staat snel te reageren op veranderingen in de markt en de behoeften van klanten.

Systemen

Exite ICT gebruikt verschillende systemen om haar diensten te leveren, zoals CRM-systemen, projectmanagementtools en monitoringtools. Deze systemen lijken goed geïntegreerd te zijn en dragen bij aan de efficiëntie en effectiviteit van het bedrijf. Er lijkt wel ruimte voor verbetering op het gebied van de implementatie van nieuwe systemen en de training van medewerkers in het gebruik ervan.

Staf (Personeel)

Exite ICT heeft een team van hoogopgeleide IT-professionals in dienst die goed presteren en betrokken zijn bij de organisatie. Het bedrijf investeert in training en ontwikkeling van medewerkers, wat leidt tot een hoog niveau van expertise en vaardigheden binnen het bedrijf. Er is echter wel een uitdaging om talent aan te trekken en te behouden in een zeer competitieve markt.

Stijl

De stijl van Exite ICT is gericht op open communicatie, samenwerking en het delen van kennis en ervaring. Het managementteam is toegankelijk en benaderbaar voor medewerkers en er heerst een informele sfeer binnen het bedrijf. Dit stimuleert medewerkers om bij te dragen aan de organisatie en zich te ontwikkelen.

Skills

De vaardigheden van Exite ICT liggen op het gebied van IT-dienstverlening, projectmanagement en consultancy. Het bedrijf heeft de expertise en vaardigheden om klanten te helpen bij het verbeteren van hun bedrijfsprocessen en het optimaliseren van hun IT-infrastructuur. Er is wellicht ruimte voor uitbreiding van het dienstenaanbod om te kunnen voldoen aan de veranderende behoeften van klanten.

Al met al lijkt Exite ICT goed gepositioneerd te zijn binnen de IT-dienstverlening met sterke punten op het gebied van shared values, strategie, structuur, systemen, staf, stijl en vaardigheden. Het bedrijf heeft echter nog wel uitdagingen, zoals het aantrekken en behouden van talent in een competitieve markt en het uitbreiden van het dienstenaanbod om te kunnen voldoen aan de veranderende behoeften van klanten.

13.5 Bijlage E: Onderzoek huidige omgeving

Doel: Onderzoek uitfasen of vervangen van Citrix omgeving, opdracht uitgebreid met licenties en overige servers

13.5.1 Citrix omgeving

De huidige Citrix omgeving bestaat uit de volgende server componenten en bevinden zich in een private cloud omgeving.

Servernaam	Rol	CPU	RAM	HDD	Opmerking
DCSF01	Delivery Controller / Storefront / License Server	2	8	100	Server 2012 R2
CTX01	Session Host	6	32	100	Server 2012 R2
CTX02	Session Host	6	32	100	Server 2012 R2
CTX03	Session Host	6	32	100	Server 2012 R2
CTX04	Session Host	6	32	100	Server 2012 R2
CTXXA01	Session Host	2	4	60	Server 2012 R2, Test server
NAG01	Citrix Gateway / Netscaler	2	8	20	T.b.v. externe toegang

Tabel 27 – Citrix omgeving

De huidige Citrix omgeving is verouderd. Op deze omgeving is Citrix XenApp 7.15 LTSR geïnstalleerd op Windows 2012 R2 servers. Citrix XenApp 7.15 is inmiddels End-of-Life en Windows 2012 R2 is na Oktober 2023 End-of-Life.

Producten welke End-of-Life zijn worden niet langer supported en ontvangen geen security updates meer.

Actieve gebruikers Citrix omgeving (moment opname)

Current User +	Name	Delivery Group	Machine Catalog	Brokering Time	Session State
CTM\jgpi	CTM\CTX01....	Windows 201...	Windows 2012 R2	6-1-2023 08:11:09	Active
CTM\jgpi	CTM\CTX01....	Windows 201...	Windows 2012 R2	5-1-2023 13:46:30	Active
CTM\jgpi	CTM\CTX02....	Windows 201...	Windows 2012 R2	5-1-2023 08:05:12	Active
CTM\jgpi	CTM\CTX03....	Windows 201...	Windows 2012 R2	2-1-2023 13:24:11	Active
CTM\jgpi	CTM\CTX03....	Windows 201...	Windows 2012 R2	6-1-2023 08:59:41	Active

Figuur 17 – Actieve Citrix omgeving

13.5.2 Gebruik Citrix en RDS Licenties

Uit de toekenning van RDS licenties blijkt dat 27 gebruikers tussen begin maart en eind april gebruik hebben gemaakt van de Citrix servers mogelijk middels Remote Desktop Services. Uit de toekenning van Citrix licenties blijkt dat 14 gebruikers in dezelfde periode gebruik hebben gemaakt van middels Citrix.

Citrix licenties

Onderstaande gebruikers hebben in de afgelopen twee maanden ingelogd op de Citrix servers.



Figuur 18 – Citrix licenties

RDS Licenties

Issued To	Issued On	Expires On
 [redacted]	maandag 5 december 2022 10:30:02	vrijdag 3 februari 2023 10:30:02
 [redacted]	dinsdag 29 november 2022 11:28:37	zaterdag 28 januari 2023 11:28:37
 [redacted]	maandag 7 november 2022 13:12:13	vrijdag 6 januari 2023 13:12:13
 [redacted]	donderdag 17 november 2022 18:56:16	maandag 16 januari 2023 18:56:16
 [redacted]	dinsdag 29 november 2022 09:06:40	zaterdag 28 januari 2023 09:06:40
 [redacted]	dinsdag 15 november 2022 08:19:44	zaterdag 14 januari 2023 08:19:44
 [redacted]	maandag 19 december 2022 08:22:55	vrijdag 17 februari 2023 08:22:55
 [redacted]	dinsdag 29 november 2022 09:50:32	zaterdag 28 januari 2023 09:50:32
 [redacted]	dinsdag 29 november 2022 15:25:46	zaterdag 28 januari 2023 15:25:46
 [redacted]	vrijdag 18 november 2022 08:41:26	dinsdag 17 januari 2023 08:41:26
 [redacted]	dinsdag 29 november 2022 15:25:30	zaterdag 28 januari 2023 15:25:30
 [redacted]	woensdag 21 december 2022 08:52:54	zondag 19 februari 2023 08:52:54
 [redacted]	maandag 5 december 2022 21:38:45	vrijdag 3 februari 2023 21:38:45
 [redacted]	woensdag 21 december 2022 12:07:55	zondag 19 februari 2023 12:07:55
 [redacted]	maandag 2 januari 2023 08:26:14	vrijdag 3 maart 2023 08:26:14
 [redacted]	woensdag 16 november 2022 13:50:37	zondag 15 januari 2023 13:50:37
 [redacted]	donderdag 24 november 2022 11:30:32	maandag 23 januari 2023 11:30:32
 [redacted]	vrijdag 23 december 2022 08:29:31	dinsdag 21 februari 2023 08:29:31
 [redacted]	dinsdag 22 november 2022 12:27:32	zaterdag 21 januari 2023 12:27:32
 [redacted]	donderdag 17 november 2022 20:24:22	maandag 16 januari 2023 20:24:22
 [redacted]	dinsdag 29 november 2022 08:38:09	zaterdag 28 januari 2023 08:38:09
 [redacted]	woensdag 9 november 2022 11:00:24	zondag 8 januari 2023 11:00:24
 [redacted]	dinsdag 20 december 2022 14:24:04	zaterdag 18 februari 2023 14:24:04
 [redacted]	vrijdag 9 december 2022 11:44:40	dinsdag 7 februari 2023 11:44:40
 [redacted]	donderdag 8 december 2022 13:59:37	maandag 6 februari 2023 13:59:37
 [redacted]	woensdag 7 december 2022 09:15:01	zondag 5 februari 2023 09:15:01
 [redacted]	woensdag 7 december 2022 01:36:56	zondag 5 februari 2023 01:36:56

Figuur 19 – RDS licenties

13.5.3 Applicaties

Op de Citrix Session Hosts, welke de virtuele desktop aanbied, zijn de volgende applicaties geïnstalleerd:

- ✗ SAP Business One Client 9.0
- ✗ Microsoft Office
- ✗ Microsoft Project 2016 Professional
- ✗ Microsoft Visio 2016 Professional
- ✗ CES EduPack 2018
- ✗ Diagram Desinger (Meesoft.com)
- ✗ ePlan
- ✗ GanttProject
- ✗ ibaAnalyzer

- ✕ PDFsam
- ✕ SCMS Client
- ✕ TortoiseSVN
- ✕ TE DesktopSAP

Business One Client wordt voornamelijk gebruikt door 5 gebruikers, deze applicatie dient als archief en raadplegen van oude informatie. Het is onduidelijk waarom gebruikers nog inloggen op de Citrix omgeving, mogelijk zijn er gebruikers die geen gebruik maken van VPN of misschien toegang moeten hebben tot applicaties welke alleen actief zijn op de Citrix servers.

SAP Business One Client

Naast de SAP client op de Citrix Session Hosts, bestaat de SAP implementatie uit de volgende servers APP01 (SQL Server SAP databases)

13.5.4 Microsoft 365 licenties

Wat betreft Microsoft licenties kan de toewijzing van licenties efficiënter worden toegekend.

Verschillende licenties kunnen worden ondergebracht onder één licentie en brengt daarmee een kosten besparing met zich mee. Tevens zijn er licenties in gebruik welke niet volledig worden ingezet zoals de Dynamics licenties.

Licentiennaam	Totaal aantal licenties	Toegewezen licenties
Azure Active Directory Premium P1	50	42
Azure Active Directory Premium P2	7	7
Dynamics 365 Finance Attach to Qualifying Dynamics 365 Base Offer	5	3
Dynamics 365 Project Operations Attach	8	3
Dynamics 365 Supply Chain Management	35	4
Dynamics 365 Team Members	10	3
Exchange Online (Abonnement 1)	18	16
Microsoft 365 Business Standard	2	2
Microsoft 365 E3	6	6
Microsoft 365-abonnement voor binnenlandse en internationale gesprekken	10	9
Microsoft 365-audiovergadering	6	6
Microsoft Azure Multi-Factor Authentication Premium Standalone	2	2
Microsoft Teams Phone Standard	9	8
Microsoft Teams Phone Standard - Virtuele gebruiker	9	1
Microsoft Teams Rooms Standard	1	1
Office 365 E3	70	70
Power BI Pro	10	5
Project Abonnement 3	7	7

Visio Abonnement 2	3	3
--------------------	---	---

Tabel 28 – Licenties

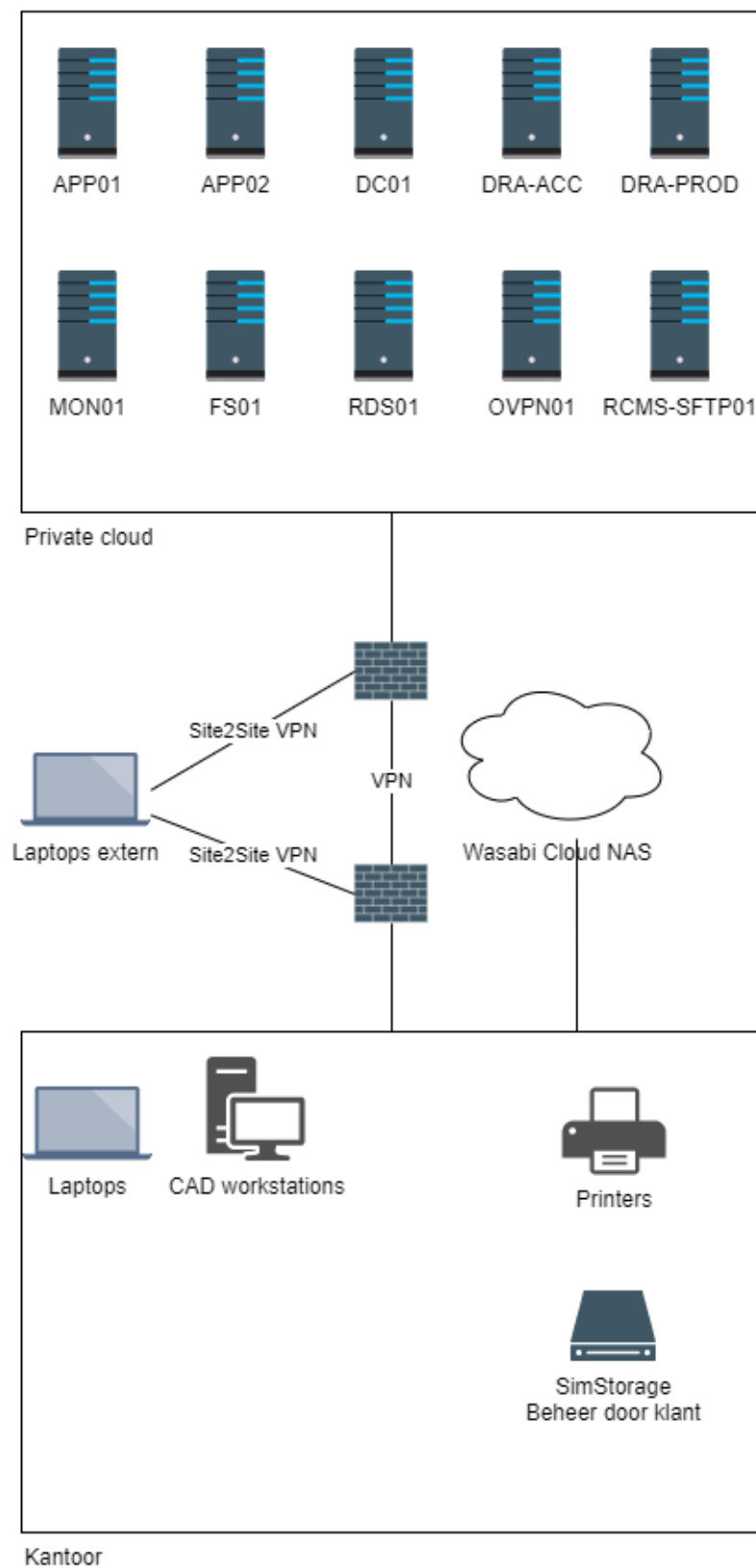
13.5.5 Overige servers met verouderde besturingssystemen

Ook voor onderstaande servers geldt dat deze van verouderde besturingssystemen gebruik maken en voor oktober 2023 vervangen moeten zijn.

Servernaam	Rol	CPU	RAM	HDD	Opmerking
APP01	SQL Server (SAP) / Exchange Management	4	32	350	SQL Server SAP, huidige memory gebruik 37% (20GB beschikbaar)
APP02	SQL Server (Stratech SPS) / SVN Server	2	8	100	SQL Server Stratech SPS
APP03	MySQL / OpenVPN / TCserver / GTP Tracker	4	4	140	D: schijf niet in gebruik
DC01	Domain Controller / Fileserver / DNS / DHCP / Radius server / eBridge MFP software (Toshiba)	2	8	3600	Shares worden aangeboden met DFS / actieve DHCP server / Radius tbv SonicWall NSA en AP's
DC02	Domain Controller / Printserver / DNS / Radius server	2	8	320	Oude Printserver, Radius tbv SonicWalls, Citrix Gateway, Fileserver tbv Citrix Profielen
MON01	Ivensys / Archestra License Manager / SQL Server / Wonderware Historian	2	4	150	Data verzameling van Turbine PCs, drivemapping naar SFTP server
PRINT01	Printserver / Toshiba eFollow	2	4	60	Printserver

Tabel 29 – Overige verouderde servers

13.6 Bijlage F: Nieuwe situatie



Figuur 20- Nieuwe situatie

Algemene Voorwaarden

1. **Toepasselijkheid**
Exite ICT (Exite) Voorwaarden, in deze algemene voorwaarden ("AV") wordt onder "Exite" verstaan: Exite ICT, statutair gevestigd te Enschede en kantoorhoudende Hengelosestraat 501, 7521 AG te Enschede en onder "wederpartij": partij met wie Exite een overeenkomst heeft gesloten.
11. De Exite Voorwaarden bestaan uit de onderhavige module Algemeen en de volgende afzonderlijke specifieke modules, die te raadplegen zijn via <https://www.exite.com> onder de map support.
111. Licentie voor programmatuur
112. Ontwikkeling van programmatuur
113. Onderhoud van programmatuur
114. Application Service Provider, Software as a Service en Computerservice
115. Ontwikkeling en onderhoud van een website
116. Webhosting
117. Detacheringsdiensten
118. Opleidingen en trainingen
119. Advisering, consultancy en projectmanagement
1110. Overige diensten
1111. Verkoop van ICT-, telecommunicatie- en kantoorapparatuur en andere zaken
1112. Verhuur van ICT-, telecommunicatie- en kantoorapparatuur
1113. Onderhoud van ICT-, telecommunicatie- en kantoorapparatuur
1114. Toegang tot internet
1115. Telecommunicatiediensten
1116. Financiering en leasing van ICT.
12. Deze module Algemeen van de Exite Voorwaarden is van toepassing op alle aanbiedingen en overeenkomsten waarbij Exite goederen en/of diensten van welke aard en onder welke benaming dan ook aan cliënt levert. Tevens zijn van toepassing de specifieke module of modules van de Exite Voorwaarden die tussen Exite en cliënt zijn overeengekomen. Indien deze module Algemeen van de Exite Voorwaarden op enig onderdeel strijdig of onverenigbaar is met het bepaalde in de tussen Exite en cliënt overeengekomen specifieke module of modules van de Exite Voorwaarden, prevaleert het bepaalde in de desbetreffende specifieke module of modules.
13. Door waar in de Exite Voorwaarden de term "algemene voorwaarden" wordt gebruikt, wordt daardoor verstaan de bepalingen van deze module Algemeen in combinatie met de bepalingen van één of meer overeengekomen specifieke modules van de Exite Voorwaarden.
14. Afwijkingen en aanvullingen van deze algemene voorwaarden zijn slechts geldig indien deze schriftelijk tussen partijen zijn overeengekomen.
15. De toepasselijkheid van inkoop- of andere voorwaarden van cliënt wordt uitdrukkelijk van de hand gewezen.
16. Indien en voor zover Exite apparatuur van derden aan cliënt levert, zullen, mits dat door Exite schriftelijk aan cliënt is meegedeeld, voor wat betreft die apparatuur de voorwaarden van die derden van toepassing zijn, met terzijdestelling van de daarvan afwijkende bepalingen in deze algemene voorwaarden. Cliënt aanvaardt de bedoelde voorwaarden van derden. Deze voorwaarden liggen voor cliënt ter inzage bij Exite en Exite zal deze aan cliënt kosteloos op zijn verzoek toezenden. Indien en voor zover de bedoelde voorwaarden van derden in de verhouding tussen cliënt en Exite om welke reden dan ook geacht worden niet van toepassing te zijn of buiten toepassing worden verklaard, geldt het bepaalde in deze algemene voorwaarden onverminderd.
17. Indien enige bepaling van deze algemene voorwaarden nietig is of vernietigd wordt, zullen de overige bepalingen van deze algemene voorwaarden onverminderd van kracht blijven. Exite en cliënt zullen in dat geval in overleg treden met het doel nieuwe bepalingen ter vervanging van de nietige of vernietigde bepalingen overeen te komen, waarbij zoveel mogelijk het doel en de strekking van de nietige dan wel vernietigde bepalingen in acht wordt genomen.
2. **Aanbiedingen**
21. Alle aanbiedingen en andere uitingen van Exite zijn vrijblijvend, tenzij door Exite schriftelijk anders is aangegeven.
22. Cliënt staat in voor de juistheid en volledigheid van de door of namens hem aan Exite verstrekte gegevens waarop deze zijn aanbieding gebaseert. Cliënt betracht steeds de uiterste zorg dat de eisen waaraan de prestatie van Exite dient te voldoen, juist en volledig zijn. In tekeningen, afbeeldingen, catalogi, websites, offertes, reclamemateriaal, normalisatiebladen e.d. vermelde maten en gegevens zijn voor Exite niet bindend, behoudens indien door Exite uitdrukkelijk anders is vermeld.
23. In de eventuele verplichting tot installatie en/of configuratie van apparatuur door Exite is niet inbegrepen het uitvoeren van dataconversie en het installeren van software.
3. **Prijs en betaling**
31. Alle prijzen zijn exclusief omzetbelasting (BTW) en andere heffingen welke van overheidswege zijn of worden opgelegd. Tenzij anders overeengekomen, zijn alle prijzen steeds in euro's en dient cliënt alle betalingen in euro's te voldoen.
32. Alle door Exite afgegeven voorcalculaties en begrotingen hebben slechts een indicatief karakter, tenzij Exite schriftelijk anders kenbaar maakt. Aan een door Exite afgegeven voorcalculatie of begroting kunnen door cliënt nimmer rechten of verwachtingen worden ontleend. Een door cliënt aan Exite kenbaar gemaakt beschikbaar budget geldt nimmer als een tussen partijen overeengekomen (vaste) prijs voor de door Exite te verrichten prestaties. Uitsluitend indien zulks tussen partijen schriftelijk is overeengekomen is Exite gehouden cliënt te informeren bij dreigende overschrijding van een door Exite afgegeven voorcalculatie of begroting.
33. Indien cliënt bestaat uit meerdere natuurlijke personen en/of rechtspersonen, is elk van die personen hoofdelijk gehouden de uit de overeenkomst verschuldigde bedragen te voldoen.
34. Ter zake van door Exite verrichte prestaties en de daarvoor door cliënt verschuldigde bedragen leveren de relevante documenten en gegevens uit de administratie of systemen van Exite volledig bewijs op, onverminderd het recht van cliënt tot het leveren van tegenbewijs.
35. Indien sprake is van een periodieke betalingsverplichting van cliënt, geldt dat Exite gerechtigd is schriftelijk op een termijn van ten minste drie maanden de geldende prijzen en tarieven aan te passen. Indien cliënt niet akkoord wenst te gaan met een dergelijke aanpassing, is cliënt gerechtigd binnen dertig dagen na de kennisgeving de overeenkomst schriftelijk op te zeggen tegen de datum waarop de aanpassing in werking zou treden. Cliënt komt zodanig recht tot opzegging echter niet toe indien tussen partijen is overeengekomen dat de geldende prijzen en tarieven worden aangepast met inachtneming van een tussen partijen overeengekomen index of andere maatstaf.
36. Partijen zullen in de overeenkomst de datum of data waarop Exite de vergoeding voor de overeengekomen prestaties aan cliënt in rekening brengt, vastleggen. Verschuldigde bedragen worden door cliënt betaald volgens de overeengekomen dan wel op de factuur vermelde betalingscondities. Bij gebreke van een specifieke regeling zal cliënt binnen een door Exite te bepalen termijn na factuurdatum betalen. Cliënt is niet gerechtigd tot opschorting of andere maatstaf.
37. Indien cliënt de verschuldigde bedragen niet of niet tijdig betaalt, is cliënt, zonder dat enige aanmaning of ingebrekestelling nodig is, over het openstaande bedrag wettelijke handelsrente verschuldigd. Indien cliënt na aanmaning of ingebrekestelling nakstig blijft de vordering te voldoen, kan Exite de vordering uit handen geven, in welk geval cliënt naast het dan verschuldigde totale bedrag tevens gehouden is tot vergoeding van alle gerechtelijke en buitengerechtelijke kosten, waaronder begrepen alle kosten berekend door externe deskundigen.
4. **Vertrouwelijkheid en overname personeel**
41. Cliënt en Exite dragen er zorg voor dat alle van de andere partij ontvangen gegevens waarvan men weet of redelijkerwijs behoort te weten dat deze van vertrouwelijke aard zijn, geheim blijven. De partij die vertrouwelijke gegevens ontvangt, zal deze slechts gebruiken voor het doel waarvoor deze verstrekt zijn. Gegevens worden in ieder geval als vertrouwelijk beschouwd indien deze door één der partijen als zodanig zijn aangeduid.
42. Cliënt zal gedurende de looptijd van de overeenkomst evenals één jaar na het einde daarvan slechts na voorafgaande schriftelijke toestemming van de andere partij, medewerkers van de andere partij die betrokken zijn of zijn geweest bij de uitvoering van de overeenkomst, in dienst nemen dan wel anderszins, direct of indirect, voor zich laten werken. Aan bedoelde toestemming kunnen voorwaarden zijn verbonden.
43. Voor iedere overtreding van het bepaalde in lid 42 zal de wederpartij aan Exite een boete betalen, welke niet voor rechterlijke motiging vatbaar is, die overeenkomt met een bedrag gelijk aan het op dat tijdstip bij Exite geldende hoogste uurtarief, verminderd met het getal 1040 (zijnde 26 weken van 40 uur per week).
5. **Privacy, gegevensverwerking en beveiliging**
51. Indien Exite dit van belang acht voor de uitvoering van de overeenkomst, zal cliënt Exite desgevraagd onverwijld schriftelijk informeren over de wijze waarop cliënt uitvoering geeft aan zijn verplichtingen op grond van wetgeving op het gebied van de bescherming van persoonsgegevens.
52. Cliënt vrijwaart Exite voor aanspraken van personen van wie persoonsgegevens zijn geregistreerd of worden verwerkt in het kader van een persoonsregistratie die door cliënt wordt gehouden of waarvoor cliënt op grond van de wet anderszins verantwoordelijk is, tenzij cliënt bewijst dat de feiten die aan de aanspraak ten grondslag liggen uitsluitend aan Exite toegerekend moeten worden.
53. De verantwoordelijkheid voor de gegevens die met gebruikmaking van een door Exite verleende dienst worden verwerkt, ligt uitsluitend bij cliënt. Cliënt staat er jegens Exite voor in dat de inhoud, het gebruik en/of de verwerking van de gegevens niet onrechtmatig zijn en geen inbreuk maken op enig recht van een derde. Cliënt vrijwaart Exite tegen elke rechtsvordering van derden, uit welke hoofde dan ook, in verband met deze gegevens of de uitvoering van de overeenkomst.
54. Indien Exite op grond van de overeenkomst gehouden is tot het voorzien in een vorm van informatiebeveiliging, zal die beveiliging beantwoorden aan de specificaties betreffende beveiliging zoals tussen partijen schriftelijk overeengekomen. Exite staat er nimmer voor in dat de informatiebeveiliging onder alle omstandigheden doeltreffend is. Indien een uitdrukkelijk omschreven beveiliging in de overeenkomst ontbreekt, zal de beveiliging voldoen aan een niveau dat, gelet op de stand van de techniek, de gevoeligheid van de gegevens en de aan het treffen van de beveiliging verbonden kosten niet onredelijk is.
55. Indien bij de uitvoering van de overeenkomst of anderszins gebruik wordt gemaakt van computer-, data- of telecommunicatiefaciliteiten is Exite gerechtigd cliënt toegangs- of identificatiecodes toe te wijzen. Exite is gerechtigd toegewezen toegangs- of identificatiecodes te wijzigen. Cliënt behandelt de toegangs- en identificatiecodes vertrouwelijk en met zorg en maakt deze slechts aan geautoriseerde personeelsleden kenbaar. Exite is nimmer aansprakelijk voor schade of kosten die het gevolg zijn van gebruik of misbruik dat van toegangs- of identificatiecodes wordt gemaakt, tenzij het misbruik mogelijk is geweest als rechtstreeks gevolg van een handelen of nalaten van Exite.
6. **Voorbehoud van eigendom en rechten, zaaksvorming en opschorting**
61. Alle aan cliënt geleverde zaken blijven eigendom van Exite totdat alle bedragen die cliënt aan Exite op grond van de tussen partijen gesloten overeenkomst verschuldigd is, volledig aan Exite zijn voldaan. Een cliënt die als medeverkoper optreedt, zal alle zaken die onderworpen zijn aan het eigendomsvoorbehoud van Exite mogen verkopen en doorleveren voor zover dat gebruikelijk is in het kader van de normale uitoefening van zijn bedrijf. Indien cliënt (mede) uit door Exite geleverde zaken een nieuwe zaak vormt, vormt cliënt die zaak slechts voor Exite en houdt cliënt de nieuw gevormde zaak voor Exite totdat cliënt alle op grond van de overeenkomst verschuldigde bedragen heeft voldaan; Exite blijft in dat geval tot het moment van volledige voldoening door cliënt eigenaar van de nieuw gevormde zaak.
62. De goederenrechtelijke gevolgen van het eigendomsvoorbehoud van een voor uitvoer bestemde zaak worden beheerst door het recht van de Staat van bestemming indien dat recht ter zake voor Exite gunstigere bepalingen bevat.
63. Rechten, waaronder made begrepen gebruiksrechten, worden in voorkomend geval aan cliënt verleend of overgedragen onder de voorwaarde dat cliënt alle uit de tussen partijen gesloten overeenkomst verschuldigde vergoedingen volledig heeft betaald. Indien partijen voor de verlening van een gebruiksrecht een periodieke betalingsverplichting van cliënt zijn overeengekomen, komt aan cliënt het gebruiksrecht toe zolang hij zijn periodieke betalingsverplichting nakomt.
64. Exite kan de in het kader van de overeenkomst ontvangen of gegenereerde zaken, producten, vermogensrechten, gegevens, documenten, programmatuur, databestanden en (tussen)resultaten van de dienstverlening van Exite onder zich houden, ondanks een bestaande verplichting tot afgifte of overdracht, totdat cliënt alle aan Exite verschuldigde bedragen heeft voldaan.
7. **Risico**
71. Het risico van verlies, diefstal, verduistering of beschadiging van zaken, producten, gegevens, documenten, programmatuur, databestanden of gegevens (codes, wachtwoorden, documentatie etc.) die in het kader van de uitvoering van de overeenkomst vervaardigd of gebruikt worden, gaat over op cliënt op het moment waarop deze in de feitelijke beschikingsmacht van cliënt of een hulppersoon van cliënt zijn gebracht. Voor zover deze objecten in de feitelijke beschikingsmacht van Exite of hulppersonen van Exite zijn, draagt Exite het risico van verlies, diefstal, verduistering of beschadiging.
8. **Rechten van intellectuele eigendom**
81. Indien Exite bereid is zich te verbinden tot overdracht van een recht van intellectuele eigendom, kan een zodanige verbintenis slechts schriftelijk en uitdrukkelijk worden aangegaan. Indien partijen schriftelijk overeenkomen dat een recht van intellectuele eigendom ten aanzien van specifiek voor cliënt ontwikkelde programmatuur, websites, databestanden, apparatuur of andere materialen, over zal gaan op cliënt, lost dit het recht of de mogelijkheid van Exite niet aan om de aan die ontwikkeling ten grondslag liggende onderdelen, algemene beginselen, ideeën, ontwerpen, algoritmen, documentatie, werken, programmeertalen, protocollen, standaarden en dergelijke, zonder enige beperking voor andere doeleinden te gebruiken en/of te exploiteren, hetzij voor zichzelf hetzij voor derden. Evenmin staat de overdracht van een recht van intellectuele eigendom het recht van Exite aan om ten behoeve van zichzelf of een derde ontwikkelingen te doen die soortgelijk of ontleend zijn aan die welke ten behoeve van cliënt zijn of worden gedaan.
82. Alle rechten van intellectuele eigendom op de op grond van de overeenkomst ontwikkelde of aan cliënt ter beschikking gestelde programmatuur, websites, databestanden, apparatuur of andere materialen zoals analyses, ontwerpen, documentatie, rapporten, offertes, evenals voorbereidend materiaal daarvan, berusten uitsluitend bij Exite, diens licentiegevers of diens toeleveranciers. Cliënt verkrijgt uitsluitend de gebruiksrechten die bij deze algemene voorwaarden en de wet uitdrukkelijk zijn toegekend. Een aan cliënt toekomend recht tot gebruik is niet-exclusief, niet-overdraagbaar aan derden en niet sub-licentiebaar.
83. Het is cliënt niet toegestaan enige concludering betreffende het vertrouwelijke karakter dan wel betreffende auteursrechten, merken, handelsnamen of enig ander recht van intellectuele eigendom uit de programmatuur, websites, databestanden, apparatuur of materialen te verwijderen of te wijzigen.
84. Ook indien de overeenkomst niet uitdrukkelijk in een bevoegdheid daartoe voorziet, is het Exite toegestaan technische voorzieningen aan te brengen ter bescherming van de programmatuur, apparatuur, databestanden, websites en dergelijke in verband met een overeengekomen beperking in de inhoud of de duur van het recht tot gebruik van deze objecten. Het is cliënt nimmer toegestaan een dergelijke technische voorziening te (laten) verwijderen of te (laten) omzeilen.
85. Exite vrijwaart cliënt tegen elke rechtsvordering van een derde welke gebaseerd is op de bewering dat door Exite zelf ontwikkelde programmatuur, websites, databestanden, apparatuur of andere materialen inbreuk maken op een recht van intellectuele eigendom van die derde, onder de voorwaarde dat cliënt Exite onverwijld schriftelijk informeert over het bestaan en de inhoud van de rechtsvordering en de afhandeling van de zaak, waaronder het treffen van eventuele schikkingen, geheel overlaat aan Exite. Cliënt zal daartoe de nodige volmachten, informatie en medewerking aan Exite verlenen om zich, indien nodig in naam van cliënt, tegen deze rechtsvorderingen te verweren. Deze verplichting tot vrijwaring vervalt indien de verweten inbreuk verband houdt (i) met door cliënt ter gebruik, bewerking, verwerking of incorporatie aan Exite ter beschikking gestelde materialen, dan wel (ii) met wijzigingen die cliënt zonder schriftelijke toestemming van Exite in de programmatuur, website, databestanden, apparatuur of andere materialen heeft aangebracht of door een derde heeft laten aanbrengen. Indien in rechte onroepelijk vaststaat dat de door Exite zelf ontwikkelde programmatuur, websites, data- bestanden, apparatuur of andere materialen inbreuk maken op enig aan een derde toebehorend recht van intellectuele eigendom of indien naar het oordeel van Exite een derde kans bestaat dat een zodanige inbreuk zich voordoet, zal Exite, indien mogelijk, zorg dragen dat cliënt het geleverde, of functioneel gelijkwaardige andere programmatuur, websites, databestanden, apparatuur of materialen kan blijven gebruiken. Iedere andere of verdergaande vrijwaringverplichting van Exite is uitgesloten.
86. Cliënt garandeert dat geen rechten van derden zijn verzetten tegen beschikbaarstelling aan Exite van apparatuur, programmatuur, voor websites bestemd materiaal (beeldmateriaal, tekst, muziek, domeinnamen, logo's, hyperlinks etc.), databestanden of andere materialen, waaronder ontwerp-materiaal, met het doel van gebruik, bewerking, installatie of incorporatie (zijv. in een website). Cliënt vrijwaart Exite tegen elke aanspraak van een derde die gebaseerd is op de bewering dat zodanig beschikbaar stellen, gebruik, bewerken, installeren of incorporeren inbreuk maakt op enig recht van die derde.
9. **Medewerkingsverplichtingen**
91. Partijen erkennen dat het wettiggen van werkzaamheden op het gebied van informatie- en communicatietechnologie in de regel afhankelijk is van een juiste en tijdige onderlinge samenwerking. Om een behoorlijke uitvoering van de overeenkomst door Exite mogelijk te maken zal cliënt Exite steeds tijdig alle door Exite nuttig, nodig en wenselijk geachte gegevens of inlichtingen verschaffen en alle medewerking verstrekken. Indien cliënt in het kader van het verlenen van medewerking aan de uitvoering van de overeenkomst eigen personeel en/of hulppersonen inzet, zullen dit personeel en deze hulppersonen beschikken over de noodzakelijke kennis, deskundigheid en ervaring.
92. Cliënt draagt het risico van de selectie, het gebruik, de toepassing en het beheer in zijn organisatie van de apparatuur, programmatuur, websites, databestanden en andere producten en materialen en van de door Exite te verlenen diensten. Cliënt zelf draagt zorg voor de juiste installatie, montage en ingebruikneming en voor de juiste instellingen van de apparatuur, programmatuur, websites, databestanden en andere producten en materialen.
93. Indien cliënt de voor de uitvoering van de overeenkomst door Exite nuttig, nodig of wenselijk geachte gegevens, documenten, apparatuur, programmatuur, materialen of medewerkers niet, niet tijdig of niet overeenkomstig de afspraken ter beschikking van Exite stelt of indien cliënt op andere wijze niet aan zijn verplichtingen voldoet, heeft Exite het recht tot gehele of gedeeltelijke opschorting van de uitvoering van de overeenkomst en heeft Exite tevens het recht om de daardoor ontstane kosten volgens zijn gebruikelijke tarieven in rekening te brengen, een en ander onverminderd het recht van Exite tot uitoefening van enig ander wettelijk en/of overeengekomen recht.

- 9.4. Ingeval medewerkers van Exite op locatie van cliënt werkzaamheden verrichten, draagt cliënt kosteloos zorg voor de door die medewerkers in redelijkheid gewenste faciliteiten, zoals een werkruimte met computer-, data- en telecommunicatiefaciliteiten. De werkruimte en faciliteiten zullen voldoen aan alle wettelijke en overige geldende eisen betreffende arbeidsomstandigheden. Cliënt vrijwaart Exite voor aanspraken van derden, waaronder medewerkers van Exite, die in verband met de uitvoering van de overeenkomst schade lijden welke het gevolg is van handelen of nalaten van cliënt of van onvrije situaties in diens organisatie. Cliënt zal de binnen zijn organisatie geldende huis- en beveiligingsregels vóór aanvang van de werkzaamheden aan de door Exite ingezetste medewerkers kenbaar maken.
- 9.5. Indien bij de uitvoering van de overeenkomst gebruik wordt gemaakt van computer-, data- of telecommunicatiefaciliteiten, waaronder internet, is cliënt verantwoordelijk voor de juiste keuze van de daarvoor benodigde middelen en voor de tijdige en volledige beschikbaarheid ervan, behoudens voor die faciliteiten welke onder direct gebruik en beheer van Exite staan. Exite is nimmer aansprakelijk voor schade of kosten wegens transmissiefouten, storingen of niet-beschikbaarheid van deze faciliteiten, tenzij cliënt bewijst dat deze schade of kosten het gevolg zijn van opzet of bewuste roekeloosheid van de directie van Exite.
- 9.6. Cliënt draagt er zorg voor dat de ruimte van de cliënt, waar Exite haar werkzaamheden verricht, waar de controles of testwerkzaamheden moeten plaatsvinden en/of waar de (op)geleverde zaken, waarop garantieverplichtingen betrekking hebben zich bevinden, in overeenstemming wordt gebracht en gehouden met de daaraan door Exite te stellen eisen van temperatuur, vochtigheidsgraad, tochtvrijheid, energie- en watervoorvoer en andere omgevingseisen.
- 10. Leveringstermijnen**
- 10.1. Alle door Exite genoemde of overeengekomen (leverings)termijnen en (oplever)data zijn naar beste weten vastgesteld op grond van de gegevens die hem bij het aangaan van de overeenkomst bekend waren. Door Exite genoemde of tussen partijen overeengekomen tussentijdse (oplever)data, gelden steeds als streefdata, binden Exite niet en hebben steeds slechts een indicatief karakter. Exite spant zich er redelijkerwijs voor in uiterste (leverings)termijnen en uiterste (oplever)data zoveel mogelijk in acht te nemen. Exite is niet gebonden aan een al dan niet uiterste (leverings)termijn of (oplever)datum, die, vanwege buiten zijn macht gelegen omstandigheden, die zich na het aangaan van de overeenkomst hebben voorgedaan, niet meer gehaald kan worden. Evenmin is Exite gebonden aan een al dan niet uiterste (oplever)datum of (leverings)termijn als partijen een wijziging van de inhoud of omvang van de overeenkomst (meiswerk, wijziging van specificaties etc.) of een wijziging van de aanpak van de uitvoering van de overeenkomst zijn overeengekomen. Indien overschrijding van enige termijn dreigt, zullen Exite en cliënt in overleg treden om de gevolgen van de overschrijding voor de verdere planning te bespreken.
- 10.2. De enkele overschrijding van een door Exite genoemde of tussen partijen overeengekomen al dan niet uiterste (leverings)termijn of (oplever)datum brengt Exite niet in verzuim. In alle gevallen - derhalve ook ingeval partijen schriftelijk en uitdrukkelijk een uiterste (leverings)termijn of (oplever)datum zijn overeengekomen - komt Exite wegens tijdsoverschrijding eerst in verzuim nadat cliënt hem schriftelijk in gebreke heeft gesteld. De ingebrekestelling dient een zo volledig en gedetailleerd mogelijke omschrijving van de tekortkoming te bevatten, opdat Exite in de gelegenheid wordt gesteld adequaat te reageren.
- 10.3. Exite is steeds gerechtigd de overeenkomst in deelleveringen uit te voeren.
- 11. Garantie**
- 11.1. Exite zal zich er naar beste vermogen voor inspannen eventuele materiaal- en fabricagefouten in de apparatuur, alsmede in onderdelen die door Exite in het kader van garantie zijn geleverd, binnen redelijke termijn kosteloos te herstellen indien deze binnen een periode van drie maanden na aflevering gedetailleerd omschreven bij Exite zijn gemeld. Indien hersteld naar het redelijk oordeel van Exite niet mogelijk is, herstel te lang gaat duren of als aan herstel onoverredig hoge kosten zijn verbonden, is Exite gerechtigd de apparatuur kosteloos te vervangen door andere, soortgelijke maar niet noodzakelijkerwijs identieke apparatuur. Dataconversie die noodzakelijk is als gevolg van herstel of vervanging, valt buiten de garantie. Alle vervangen onderdelen worden eigendom van Exite. De garantieverplichting vervalt indien fouten in de apparatuur of in de onderdelen geheel of gedeeltelijk het gevolg zijn van onjuist, onzorgvuldig of ondeskundig gebruik, van buiten komende oorzaken zoals brand- of waterschade, of indien cliënt zonder toestemming van Exite wijzigingen in de apparatuur of in de onderdelen die door Exite in het kader van garantie zijn geleverd, aanbrengt of kaot aanbrengen. Exite zal een zodanige toestemming niet op onredelijke gronden onthouden.
- 11.2. Ieder ander of verdergaand beroep van cliënt op non-conformiteit van de geleverde zaken dan het bepaalde in artikel 8.1 van deze module is uitgesloten. Cliënt mag zich in ieder geval niet beroepen op de non-conformiteit van de geleverde zaken indien en voor zover de wet hem dat beroep ontzegt.
- 11.3. Kosten van werkzaamheden en herstel buiten het kader van deze garantie zullen door Exite in rekening worden gebracht conform zijn gebruikelijke tarieven.
- 11.4. Exite heeft geen verplichting tot herstel van fouten die na afloop van de in artikel 11.1 bedoelde garantperiodes zijn gemeld, tenzij tussen partijen een onderhoudsovereenkomst is afgesloten welke een zodanige plicht tot herstel omvat.
- 12. Ontbinding en opzegging van de overeenkomst**
- 12.1. Aan elk der partijen komt de bevoegdheid tot ontbinding van de overeenkomst wegens een toerekenbare tekortkoming in de nakoming van de overeenkomst slechts toe indien de andere partij, steeds in alle gevallen na een zo gedetailleerd mogelijke schriftelijke ingebrekestelling waarbij een redelijke termijn gesteld wordt voor zuivering van de tekortkoming, toerekenbaar tekortschiet in de nakoming van wezenlijke verplichtingen uit de overeenkomst. Betalingsverplichtingen van cliënt en alle andere verplichtingen tot medewerking door de cliënt of een door de cliënt in te schakelen derde gelden steeds als wezenlijke verplichtingen uit de overeenkomst.
- 12.2. Indien cliënt op het moment van de ontbinding als bedoeld in artikel 11.1 reeds prestaties ter uitvoering van de overeenkomst heeft ontvangen, zullen deze prestaties en de daarmee samenhangende betalingsverplichting geen voorwerp van ongedaan making zijn, tenzij cliënt bewijst dat Exite ten aanzien van het wezenlijke deel van die prestaties in verzuim is. Bedragen die Exite vóór de ontbinding heeft gefactureerd in verband met hetgeen hij ter uitvoering van de overeenkomst reeds naar behoren heeft verricht of geleverd, blijven met inachtneming van het in de vorige paragraaf bepaalde onverminderd verschuldigd en worden op het moment van de ontbinding direct opeisbaar.
- 12.3. Indien een overeenkomst welke naar zijn aard en inhoud niet door volbrenging eindigt, voor onbepaalde tijd is aangegaan, kan deze door elk der partijen na goed overleg en onder opgave van redenen schriftelijk worden opgezegd. Indien tussen partijen geen opzegtermijn is overeengekomen, dient bij de opzegging een redelijke termijn in acht te worden genomen. Partijen zullen wegens opzegging nimmer tot enige schadevergoeding zijn gehouden.
- 12.4. Cliënt is nimmer gerechtigd een overeenkomst van dienstverlening of van opdracht welke voor bepaalde tijd is aangegaan, tussentijds op te zeggen.
- 12.5. Elk der partijen kan de overeenkomst zonder ingebrekestelling met onmiddellijke ingang geheel of gedeeltelijk schriftelijk opzeggen indien de wederpartij - al dan niet voorlopig - surseance van betaling wordt verleend, indien ten aanzien van de andere partij faillissement wordt aangevraagd, indien de onderneming van de andere partij wordt geliquideerd of beëindigd anders dan ten behoeve van reconstructie of samenvoeging van ondernemingen, of indien de beslissende zeggenschap over de onderneming van cliënt wijgt. Exite is wegens deze beëindiging nimmer tot enige restitutie van reeds ontvangen gelden dan wel tot schadevergoeding gehouden. Ingeval van faillissement van cliënt vervalt het recht tot gebruik van aan cliënt ter beschikking gestelde programmatuur, websites en dergelijke van rechtswege.
- 13. Aansprakelijkheid van Exite**
- 13.1. De totale aansprakelijkheid van Exite wegens een toerekenbare tekortkoming in de nakoming van de overeenkomst of uit enige andere hoofde, daaronder uitdrukkelijk ook begrepen iedere tekortkoming in de nakoming van een met cliënt overeengekomen garantieverplichting, is beperkt tot vergoeding van directe schade tot maximaal het bedrag van de voor die overeenkomst bedongen prijs (excl. BTW). Deze beperking van aansprakelijkheid is van overeenkomstige toepassing op de in artikel 8.5 van deze module Algemeen bedoelde vrijwaringsverplichting van Exite. Indien de overeenkomst hoofdzakelijk een duurovereenkomst is met een looptijd van meer dan één jaar, wordt de voor de overeenkomst bedongen prijs gesteld op het totaal van de vergoedingen (excl. BTW) bedongen voor één jaar. In geen geval zal de totale aansprakelijkheid van Exite voor directe schade, uit welke hoofde dan ook, echter meer bedragen dan € 500.000 (vijfhonderd duizend Euro).
- 13.2. De aansprakelijkheid van Exite voor schade door dood, lichamelijk letsel of wegens materiële beschadiging van zaken bedraagt totaal nimmer meer dan € 1250.000 (één miljoen tweehonderdvijftig duizend Euro).
- 13.3. De aansprakelijkheid van Exite voor indirecte schade, gevolgschade, gederfde winst, gemiste besparingen, verminderde goodwill, schade door bedrijfsstagnatie, schade als gevolg van aanspraken van afnemers van cliënt, schade verband houdende met het gebruik van door cliënt aan Exite voorgeschreven zaken, materialen of programmatuur van derden en schade verband houdende met de inschakeling van door cliënt aan Exite voorgeschreven toeleveranciers is uitgesloten. Eveneens is uitgesloten de aansprakelijkheid van Exite wegens vernieling, vernietiging of verlies van gegevens of documenten.
- 13.4. De uitsluitingen en beperkingen van de aansprakelijkheid van Exite, zoals omschreven in de voorgaande leden van dit artikel 12, laten de overige uitsluitingen en beperkingen van aansprakelijkheid van Exite uit hoofde van deze module Algemeen en de overige overeengekomen modules van deze algemene voorwaarden geheel onverlet.
- 13.5. De in artikel 12.1 tot en met 12.4 bedoelde uitsluitingen en beperkingen komen te vervallen indien en voor zover de schade het gevolg is van opzet of bewuste roekeloosheid van de directie van Exite.
- 13.6. Tenzij nakoming door Exite blijvend onmogelijk is, ontstaat de aansprakelijkheid van Exite wegens toerekenbare tekortkoming in de nakoming van een overeenkomst slechts indien cliënt Exite onverwijld schriftelijk in gebreke stelt, waarbij een redelijke termijn voor de zuivering van de tekortkoming wordt gesteld, en Exite ook na die termijn toerekenbaar blijft tekortschieten in de nakoming van zijn verplichtingen. De ingebrekestelling dient een zo volledig en gedetailleerd mogelijke omschrijving van de tekortkoming te bevatten, opdat Exite in de gelegenheid wordt gesteld adequaat te reageren.
- 13.7. Voorzwaar voor het ontstaan van enig recht op schadevergoeding is steeds dat cliënt de schade zo spoedig mogelijk na het ontstaan daarvan schriftelijk bij Exite meldt. Iedere vordering tot schadevergoeding tegen Exite vervalt door het enkele verloop van vierentwintig maanden na het ontstaan van de vordering.
- 13.8. Partijen erkennen dat het actief en constructief deelnemen aan een ICT-Mediation een redelijke en passende maatregel is om dreigende schade te voorkomen of te beperken indien deze dreigende schade verband houdt met het niet, niet tijdig of niet behoorlijk nakomen van enige contractuele verplichting door Exite. Cliënt verplicht zich om die reden op eerste schriftelijk verzoek van Exite onverwijld actief, constructief en onvoorwaardelijk deel te nemen aan een ICT-Mediation overeenkomstig het ICT-Mediation Reglement van de Stichting Geschillenoplossing Automatisering, statutair gevestigd te Den Haag (zie <https://www.sgoa.nl>).
- 13.9. Cliënt vrijwaart Exite voor alle aanspraken van derden wegens productaansprakelijkheid als gevolg van een gebrek in een product of systeem dat door cliënt aan een derde is geleverd en dat mede bestond uit door Exite geleverde apparatuur, programmatuur of andere materialen, tenzij en voor zover cliënt bewijst dat de schade is veroorzaakt door die apparatuur, programmatuur of andere materialen.
- 13.10. Het bepaalde in dit artikel alsmede alle andere beperkingen en uitsluitingen van aansprakelijkheid genoemd in deze algemene voorwaarden gelden mede ten gunste van alle (rechts)personen waarvan Exite zich bij de uitvoering van de overeenkomst bedient.